1

AR-008-908

DSTO-TASK-R-0002

Trends in C3 System Technology

K. Fairs

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

Trends in C3 System Technology

K. Fairs

Electronics and Surveillance Research Laboratory

ABSTRACT

Task Report

This paper gives an overview of technologies considered pertinent to Command, Control and Communications (C3) systems within the next 15 years. The style of the document is tailored deliberately for the non-specialist community. The report draws primarily from research being conducted within DSTO, and mentions significant world trends. The report discusses significant near-term issues influencing C3 system design. It proposes the functionality and architecture for a future C3 system, and then maps the technologies which could support migration to such a proposed future C3 system.

Approved for public release

DSTO-Task-Report-0002

DEPARTMENT OF DEFENCE

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

Published by

Electronics and Surveillance Research Laboratory
DSTO Salisbury
Salisbury SA 5108

Telephone: (08) 259 5555
Fax: (08) 259 6980

AR No. 008-908
July 1994

APPROVED FOR PUBLIC RELEASE

CONTENTS

SECTION 1
EXECUTIVE SUMMARY

SECTION 2
INTRODUCTION

SECTION 3
SIGNIFICANT ISSUES INFLUENCING C3 SYSTEMS IN THE NEAR TERM

SECTION 4
VISION OF FUTURE C3 SYSTEMS

SECTION 5
TRENDS IN C3 SYSTEMS TECHNOLOGIES

SECTION 6
CONCLUSIONS

FIGURES

ACKNOWLEDGMENTS

This report has been possible through the ideas, comments and constructive criticisms from a number of people across the Defence Organisation who have contributed their time and energies willingly and freely. Where appropriate, text has been taken from the TTCP paper titled *C3 Technology Trends for Coalition Forces* published in March 1994. Contributors who deserve particular mention are Dr Janet Aisbett, Dr Mark Anderson, Fulvio Bagliani, Bill Blair, Lt Col Duncan Byrne, Dr David Cartwright, Dr Jennie Clothier, Dr Stephen Crawley, Dr Richard Davis, David Fogg, Lt Col John Glenn, Dr Stephen Hood, Ian Lacey, Hugh Mackenzie, Dr Gary Newsam, Brad Noakes, Dr George Poropat, Rudi Vernik, Cliff White, Dr Bob Williams and Eric Youle.

ABBREVIATIONS

ACP	Allied Communications Publication
A/D	Analog-to-Digital
ADF	Australian Defence Force
ADFCCISP	ADF Command & Control Information Systems Plan
ADFORMS	Australian Defence Force Formatted Message System
ADMI	Area of Direct Military Interest
AFCEA	Armed Forces Communications and Electronics Association
AFMC	Air Force Material Command (US)
AI	Artificial Intelligence
AIM	ADFORMS Interface Machine
ANSI	American National Standards Institute
API	Application Programming Interface
ARPA	Advanced Research Projects Agency
ASICs	Application-Specific Integrated Circuits
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
B-ISDN	Broadband- Integrated Services Digital Network
BDA	Battle Damage Assessment
BFN	Beam Forming Networks
C2I	Command and Control and Intelligence
C2RM	Command and Control Reference Model
C3	Command, Control and Communications
C4I	Command and Control, Communications-Computer and Intelligence
CAD	Computer Aided Design
CASE	Comı ıter Aided Software Engineering
CCIS	Command and Control Information System

CD-ROM	Compact Disk - Read Only Memory
CDE	Common Desk-top Environment
CINC	Commander-In-Chief
CISC	Complex Instruction Set Computer
CMW	Compartmented Mode Workstation
CNN	Cable Network News
CORBA	Common Object Request Broker Architecture
COSE	Common Operating System Environment
COTS	Commercial-Off-The-Shelf
CRT	Cathode Ray Tube
CSCW	Computer Supported Collaborative Working
CSS	Command Support System
DAI	Distributed Artificial Intelligence
DARPA	Defense Advanced Research Projects Agency
dB	decibel
DBMS	Database Management System
DCE	Distributed Computing Environment
DGPS	Differential Global Positioning System
DoD	Department of Defense
DORIC	Defence ORganisation Integrated Communications (Aust)
DOS	Disk Operating System
DPI	Dots Per Inch
DRAM	Dynamic RAM
DST	Decision-Support Template
DTM	Distributed Transaction Manager
EA	Evolutionary Acquisition
ECC	Error Correcting Codes
EEPROM	Electrically Erasable Programmable Read Only Memory
EHF	Extremely High Frequency (30 GHz - 300 GHz)
FDDI	Fibre Distributed Data Interface
FIPS	Federal Information Processing Standards

FY	Financial Year
Gb	Giga (10^{12}) bit
GIS	Geographic Information System
GOSIP	Government OSI Profile
GPS	Global Positioning System
GUI	Graphical User-interface
HAD	Heterogeneous Autonomous Distributed
HCI	Human-Computer Interaction
HDT	High Definition Television
HF	High Frequency (3 MHz - 30 MHz)
HMD	Head Mounted Displays
I/O	Input/Output
IBM	International Business Machines
IEEE	Institute of Electrical and Electronics Engineers
IFF	Identification Friend or Foe
IMINT	Image Intelligence
IN	Intelligent Networks
INMILSAT	INternational MILitary SATellite
IR	Infra Red
IS	Information Systems
ISO	International Standards Organisation
ISP	International Standard Profile
IT	Information Technology
JFAS	Jindalee Facility Alice Springs
JORN	Jindalee Operational Radar Network
JPEG	Joint Photographic Experts Group
Kb/s	Kilo (10^3) bits per second

LAN	Local Area Network
LCD	Liquid Crystal Display
LDR	Low Data Rate
LEO	Low Earth Orbit
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
MANPRINT	MANpower and PeRsonnel INTegration
Mb/s	Mega (10^6) bits per second
MB	Mega (10^6) byte
MBA	Multiple Beam Antennas
MHS	Message Handling System
MLS	Multi-Level Security
MLV	Medium Launch Vehicle
MMW	Microwave Milli-metric Wave
MOE	Measure of Effectiveness
MOP	Measures of Performance
MPEG	Moving Picture Experts Group
NATO	North Atlantic Treaty Organisation
NCSC	National Computer Security Centre (US)
NIST	National Institute of Standards and Technology
OA	Office Automation
OI	Operational Information
OIMP	Operational Information Master Plan
OLE	Object Link Embedding
OMG	Object Management Group
OS	Operating System
OSF	Open Software Foundation
OSI	Open System Interconnection
OTHR	Over The Horizon Radar
PC	Personal Computer

PGM	Precision Guided Munitions
PiGUI	Platform independent GUI
PIN	Personal Identification Number
POM	Program Objective Memorandum (US)
POSIX	Portable Operating System Interface for Computers
PTN	Personal Telecommunications Number
R&D	Research and Development
RAID	Redundant Array of Inexpensive hard disk Drives
RAM	Read Only Memory
RF	Radio Frequency
RISC	Reduced Instruction Set Computing
RPC	Remote Procedure Call
SAR	Synthetic Aperture Radar
SGML	Standard General Mark-up Language
SHF	Super High Frequency (3 GHz - 30 GHz)
SMC	Space & Missile Centre
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SRAM	Static RAM
SSCN	Secure Survivable Communications Network (US)
TTCP	The Technical Co-operation Program
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency (300 MHz - 3 GHz)
UIMS	User-interface Management System
UPC	Universal Personal Communication
US	United States
VAR	Value Added Reseller
VCI	Virtual Channel Indicator

VHF	Very High Frequency
VPI	Virtual Path Indicator
VPN	Virtual Private Network
VR	Virtual Reality
WORM	Write Once Read Many

SECTION 1
EXECUTIVE SUMMARY

1.1 Purpose

The aim of this paper is to give an overview of technologies which are considered pertinent to Command, Control and Communication (C3) systems within the next 15 years. The paper is both a stand-alone document and the Australian contribution to a joint TTCP (The Technical Co-operation Program) STP 9 (C3 Systems Technology Panel) paper titled *C3 Technology Trends for Coalition Forces* which was published in March 1994.

An objective of this document is to give a succinct appraisal of significant C3 system technologies. The style and content of the document are deliberately tailored for a non-specialist audience.

1.2 Background

The end of the Cold War in the late 1980s and follow on period of the early 1990s have been a time of immense change in the global security environment. There have been dramatic improvements in relations between the US and former Soviet bloc countries. The threat of superpower confrontation has all but disappeared. This change in strategic balance has already manifested itself in the Asia-Pacific region, an area that is fundamental to Australia's economic future. The US is working towards a more co-operative style of strategic leadership in which its allies take an increasing share of the military burden. This will increase the pressure on Australia, one of the strongest military powers in the region, to do more in its own part of the world.

New threats have emerged with the breakup of the Warsaw Pact and the end of the Cold War. They arise from the spread of advanced technology, nuclear, biological, and chemical weapons to potential Third World adversaries; aggression by major regional powers, or ethnic and religious conflicts; and potential failure of democratic reform in the former Soviet Union or elsewhere. A country's security can also be threatened by more than just direct military action. It can be degraded by a whole gambit of economic, political and social attacks. Examples would be terrorism, piracy, dumping of hazardous waste, drug-trafficking and uncontrolled flow of refugees. In dealing with many of these type of situations, the military could be required to play a significant role. The region of Australian defence interest has many of the ingredients for uncertainties which may require military presence, assistance or intervention. There is now an era of new dangers and Australia's defence planners face a period of growing complexity and uncertainty.

Modern and effective C3 systems are essential for successful prosecution of any military operation and are a significant force multiplier. Australia's use of advanced technology will continue to be a key element in the country's overall approach to its defence. This reflects the realities of a small population defending a large area, as well as the ADF's technical capacity to use advanced equipment.

1.3 Conclusions

1.3.1 General

The next 15 years will be a period of rapid change for C3 systems. The time between significant advances in hardware and software will continue to decrease. Current Information Technology (IT) systems are often obsolete within three years. Future C3 systems must be allowed to evolve continuously in order to take advantage of technology advances and for Australia to maintain a technological superiority. It is envisaged that the infrastructure for future C3 systems will be largely based on Commercial-Off-The-Shelf (COTS) products. This infrastructure may offer a richer functionality than strictly required for military purposes and will host special-to-battlefield functions as required. The open COTS product market will also enable a potential adversary to exploit such products in threat systems. Hence there should be a shift from the goal of purely a *technology superiority*. The challenge in an open COTS market is to develop smart applications supported by this advanced technology to strive for a *capability superiority*.

1.3.2 Key Requirements of Future C3 Systems

Modern joint warfare concepts mandate the need for an integrated Navy, Army, Air Force unified command. The ADF will be expected to be able to work closely with many other Government organisations and allies. Interoperability will be a key issue in enabling such diverse organisations to work together. The corner-stone of achieving interoperability will be standards. However, acquiring systems which meet the right standards is an extremely complex issue in view of the general lag of standards behind technological advances and the almost transient nature of standards. Hence, standards will be a challenge for C3 systems for the foreseeable future.

Technologies are emerging which will enable: applications to be constructed, run and maintained on multiple dissimilar platforms; and object-based applications to be constructed, run and changed on multiple platforms. The key technologies are Middleware and Distributed Object Management. The Open Software Foundation's (OSF) Distributed Computing Environment (DCE) is an emerging middleware standard on which many products are based. It will provide cross-platform interoperability so that information and processes can be shared by platforms of a dissimilar nature. Distributed Object Management will permit distributed application integration. The Object Management Group's (OMG) Common Object Request Broker Architecture (CORBA) specifies the criteria for distributed object management. It will enable applications to be constructed easily and will make use of the platform interoperability provided by DCE.

The most basic requirement will be for interoperable communication systems. Asynchronous Transfer Mode (ATM) is the switching technology which is the basis of Broadband-Integrated Services Digital Network (B-ISDN). B-ISDN will be used for global civil communications before the end of this decade. It is logical that the military should also adopt this standard. However, because B-ISDN has a commercial pedigree, it will require some militarisation. Co-ordination of the militarisation of the ATM standard will be an essential but politically difficult task which must be achieved as a fundamental building block to multi-national interoperability.

A commander's understanding of a situation is fundamental to his ability to plan, react and make good decisions. Therefore a fundamental requirement of a C3 system is to provide a full and accurate situation display. For effective operations, this common picture must be shared at all levels of the organisation and, if part of multi-national operations, by all national commanders. As with many C3 issues, although a technically difficult challenge, the ultimate limitation will be at the organisational and political levels.

1.3.3 Security

A limiting issue that will dictate the interoperability achievable among C3 systems in the next 10-15 years will be communications and computer security. The situation is becoming more complex with the introduction of greater connectivity and distributed systems. Multi-Level Security (MLS) is part of the answer and although vendors claim products to support MLS are just on the horizon, the US Command and Control, Communications - Computer and Intelligence (C4I) for the Warrior program does not envisage full MLS operation until 2010. Incremental solutions, however, are available. While there are problems with existing MLS systems (e.g. administration, audit, user-interfaces, etc.), the R&D community is working on efforts to enhance the capabilities and performance of MLS products.

Challenges will arise when multi-national MLS systems are to be inter-connected. Unless all systems are considered to afford the same level of trust by all, then information sharing will fall to the lowest common denominator of security classification. Joint certification of levels of trust of national systems will be a time-consuming and politically complex task.

With the growing dependence on IT-based C3 systems for effective military operations, these systems will be an attractive target to any enemy who may attack either physically or computer-based (logically). Measures must be taken to protect against such attacks and, in particular, overall system design must avoid a single point-of-failure that could disable the entire system.

1.3.4 C3 System Procurement

The current approval process for C3 system procurements is based on the waterfall method where project requirements are specified up-front, systems are procured and maintained for their useful life before finally being disposed of. It will require a significant change in culture to accept that a system will be permitted to evolve and grow over time. Evolutionary Acquisition (EA) is a project management process which supports incremental acquisition and development. It can significantly reduce a project's exposure to cost, schedule and technical risk. However, one thing EA cannot do is specify the total costs at the beginning of the project. Therefore EA presents a challenge within the current approval process. Although there are currently two major projects in the initial phases of acquisition which are embracing many of the principles of EA, more work needs to be done to assist in its wider acceptance by procurement authorities.

In view of the uncertainties in future conflict settings, the identification of user requirements for C3 systems to support command and control is consequently speculative. However, experience and recent evidence suggests that an infrastructure embodying a core functionality can be defined and that this infrastructure can host a useful range of applications. Rapid prototyping using this infrastructure and the advanced development environments now becoming available should decrease the cost of this activity. While the infrastructure approach should provide important stability in the procurement process and facilitate the development of user requirements (e.g. by rapid prototyping in the application layer), problems in system testing and acceptance are likely to remain.

Traditionally the intelligence community has worked behind closed doors. Intelligence collection, analysis techniques, information processing and distribution systems – due to their sensitivity, all are veiled in secrecy. There is growing recognition that intelligence system requirements are in many ways similar to C3 systems requirements and hence many of the technologies required to support them are the same. Therefore future procurement of support for C3 and intelligence systems should exploit commonality and avoid duplicated effort.

The coming generation of C3 system users are more likely to be computer-literate. There are two areas that can exploit this resource. First, future C3 systems should engage the computer-smart user in the procurement process. Not only should this engagement assist in procuring a better product but also lead to greater sense of ownership and hence system acceptance by the user. Second, future C3 systems should have facilities to support user developed software. User developed software goes beyond allowing the user to customise an interface but allows generation of high level code to optimise use of a system. However, a note of caution if user developed software is supported, the commander must retain control to manage the degree to which the user may influence the system to ensure overall performance is not impaired.

1.3.5 Communications and Networking

Communications networks are increasing in complexity and scope. They are providing a diversity of services, growing in capacity and are incorporating increased intelligence. These trends are increasing the risk of network failure arising from either errors in the design of the network software or from deliberate attack. In addition, the consequences of the failure on the network's users is likely to be more severe than in the past. At high transmission rates, networks will become large buffers which can easily become congested unless something is done to control this data latency. Network behaviour, both under normal conditions and under stress, is becoming more difficult to understand and even more difficult to predict. In particular, prediction of peak transient conditions will be vital. The current difficulties in the management, accurate modelling, and simulation of networks will be much greater with the new networks. In future conflict, military networks will rely greatly on existing commercial infrastructure and as a result, there will be increased problems concerning security control of network resources.

Future C3 systems will be based on multi-media and distributed computing technologies. In order to function in a timely manner, these technologies must be supported by high bandwidth communications. An ideal C3 system would have the same architecture from high-level strategic areas to the lowest-level tactical fighting unit. Fixed optical fibre holds the potential for virtually unlimited bandwidth but beyond line-of-site communications to support the Mobile Commander will be either narrow band or extremely expensive. The problem may be mitigated by advances in HF (High Frequency) modems (to improve throughput), cheaper more-mobile tropospheric scatter, satellite communications systems, more efficient traffic management, multiplexing techniques and compression algorithms. In reality, however, communications bandwidth at the tactical level is going to be a limited and precious resource. Hence the operational/tactical interface has the potential to become an information bottleneck.

Network management and administration of future distributed systems will be a formidable technical challenge. Even basic issues such as software updates, fault isolation, work-around and recovery of geographically dispersed systems will be problematic. Unless progress is made in resolving some of these relatively mundane issues, future C3 systems are likely to be little more than pipe-dreams and unusable in the real world.

1.3.6 Decision-Support

COTS products are just beginning to emerge which address collaborative and group working. To date, IT-assisted planning and decision-making in the C3 environment has been performed by users working independently. Now products such as Lotus Notes are allowing group preparation of planning documents. There is likely to be a proliferation of COTS group-ware products in the coming years. To be fully interoperable in a joint and multi-national environment, these common products should be adopted. Another related challenge will be translating existing planning aids from single-user environments into multi-user systems.

While there have been significant improvements in collecting data for intelligence purposes, the analysis of these data has been largely manual. This factor may have contributed to the lack of timely intelligence at the tactical level in the 1991 Gulf War. Research has provided evidence of the value of expert system techniques for intelligence processing and analysis in a conventional conflict setting and work is now being extended to a wider range of settings.

1.3.7 Multi-national C3 System Test Capability

The Gulf War proved the power and utility of a well-organised multi-national force. Fundamental to the success of this operation was an effective multi-national C3 system. The interoperation of computer based C3 systems presents many challenges not least interoperability of standards and security issues. Many of these systems-level issues were identified during the Gulf War and are now being addressed. A multi-national test environment for C3 systems, supported by real communications, is high priority requirement to support further research in this area. TTCP is well placed to co-ordinate the development and operation of such a multi-national test capability.

1.3.8 Training

The most effective training for C3 staff is to use the actual systems they would use in a real situation – future C3 systems should have access to realistic scenarios. The challenge becomes more complex when multi-national operations are considered. Distributed war-gaming across national boundaries will be required for effective training.

For the foreseeable future an integral component of all C3 systems will be the human operator. Computers which have genuine intelligence and the ability to learn, if achievable, are many years from fruition. As systems develop and become more complex, the limiting factor will increasingly be the human-machine interface. Systems of the future must have interfaces which require little or no training and are intuitive to use. Ways to improve the representation of information must be developed. Tools to navigate and seek out information intuitively are high priority requirements. Virtual reality systems offer promise in this field. These and other Human-Computer Interaction (HCI) issues will take greater prominence along with the increasing complexity of C3 systems.

SECTION 2
INTRODUCTION

2.1 Purpose

The aim of this paper is to give an overview of technologies which are considered pertinent to Command, Control and Communication (C3) systems within the next 15 years. The paper is both a stand-alone document and the Australian contribution to a joint TTCP (The Technical Co-operation Program) STP 9 (C3 Systems Technology Panel) paper titled *C3 Technology Trends for Coalition Forces* published in March 1994.

An objective of this document is to give a succinct appraisal of significant C3 system technologies. The style and content of the document are deliberately tailored for a non-specialist audience.

2.2 Scope

This paper considers a C3 system to be the arrangement of personnel, equipment, communications and procedures employed by a military Commander in the planning, directing, co-ordinating and controlling of forces and operations in the accomplishment of a mission. Although the paper addresses C3 systems technologies applicable to all levels, that is, from the Chief of the Defence Force (CDF) to the smallest fighting unit, there is an emphasis on the higher levels, where future technologies are expected to have a particularly dramatic impact.

The intention is for this paper to give an Australian perspective of trends in C3 system technologies. Hence it primarily draws from research being conducted within DSTO. Mention is made also of world-wide trends which may not currently be addressed by DSTO, where it is considered these developments could potentially be exploited by the Australian Defence Force (ADF).

While sensors are an integral part of a C3 system, this paper has been limited to a very general discussion of sensors and an overview of sensors systems likely to have a significant impact on future ADF C3 systems.

Procurement issues, although outside the scope of this paper, are discussed. This is in recognition of the fact that procurement is a significant factor in the capacity of C3 systems being able to evolve to accommodate dynamic user requirements.

2.3 Structure

The body of this paper is structured into three principal sections: Section 3, titled *Significant Issues Influencing C3 Systems in the Near Term* which sets the scene by discussing the ADF operational environment and some key issues in C3 system design and implementation: Section 4, titled *Vision of Future C3 Systems* aims to give a broad definition of the architecture and capabilities of a goal C3 system: Section 5, titled *Technology Directions*, which outlines technology trends that will support the move towards the C3 system defined in the previous section; and conclusions from the appraisal are presented in Section 6.

This report is an amalgamation of unpublished contributions given freely by technical experts from within DSTO. Information taken from published sources is referenced in the text.

SECTION 3
SIGNIFICANT ISSUES INFLUENCING C3 SYSTEMS IN THE NEAR TERM

3.1 Operational Environment

3.1.1 Australian Defence Priorities

Australia's current defence priorities were forged in the *Defence of Australia 1987* White Paper *(Reference 1)*. A review conducted in 1989 (*Australia's Strategic Planning in the 1990s – ASP 1990*) *(Reference 2)* reaffirmed the general direction of defence planning. However, the end of the Cold War has now brought about a fundamental change in the global strategic balance. This change in strategic balance has already manifested itself in the Asia-Pacific region, an area fundamental to Australia's economic future. Australia's defence planners face a period of growing complexity and uncertainty.

The *Strategic Review 1993 (Reference 3)* reflects this period of remarkable global change and uncertainty. However, the primary Defence task remains to ensure that national life is unconstrained by either direct military threat or more indirect pressures on Australian security interests. This Review also stresses the growing opportunities and need for closer relations between defence and the wider community to enhance Australia's capacity for self-reliant defence.

The end of the Cold War in the late 1980s and follow-on period of the early 1990s has been a time of immense change in the global security environment. The threat of superpower confrontation has all but disappeared. Despite the dramatic improvements in relations between the US and former Soviet bloc countries, there has been no immediate change to Australia's security environment. In the medium term, reduced superpower tensions are being translated into reduced defence budgets. The United States (US) is working towards a more co-operative style of strategic leadership in which its allies take an increasing share of the military burden. This will increase the pressure on Australia, one of the strongest military powers in the region, to do more in its own part of the world.

The *Strategic Review 1993* identifies modern and effective C3 systems as essential for successful prosecution of any military operation. As well, the Review states the ADF requires reliable and resilient C3 systems at the strategic, operational and tactical levels. C3 systems are regarded as significant force multipliers. Australia's use of advanced technology will continue to be a key element in the country's overall approach to its defence. This reflects the realities of a small population defending a large area, as well the ADF's technical capacity to use advanced equipment. The Review stresses the need to use "the most advanced capabilities in the areas such as command and control".

3.1.2 Flexibility

A country's security can be threatened by more than direct military action. For example it can be degraded by a whole gambit of economic, political, religious and social attacks. Examples would be terrorism, piracy, dumping of hazardous waste, drug-trafficking, uncontrolled flow of refugees (political and economic), pollution (marine and atmospheric), and over-exploitation of minerals and resources (such as fish, fresh water). In dealing with many of these type of threats, the military could be required to play a significant role.

Consequently, the region of Australian defence interest has many ingredients for uncertainties which may require military assistance or intervention. In the coming decade Australian is likely to face new threats which are currently evolving and, most importantly from the strategic planner's perspective, are highly unpredictable. Since the exact nature of military intervention cannot be predicted, command and control systems and supporting communications networks of the future must be flexible to adapt to any scenario.

3.1.3 Joint Operations

There is growing recognition that operations in the future are unlikely to be conducted within a single service. The *Strategic Review 1993* states that to optimise the ADF's effectiveness it is a priority to develop and exercise joint capabilities, and to plan and conduct joint ADF activities. This emphasis on joint (tri-service) operations is underlined by the current plans to co-locate the single service operational Headquarters, presently in separate establishments, together in the Sydney area. It is expected that co-location will be achieved before the end of the decade.

3.1.4 Multi-national Operations

Most military strategists agree Australia is very unlikely to conduct major off-shore operations as a single country. Future overseas deployments are more likely to be as part of a larger multi-national force, probably organised under the auspices of the UN. The exact make-up of such a multi-national force will be difficult to define in advance. The 1991 Gulf War provided an extraordinary example of such a multi-national force – 38 countries actively participated, with another 4 contributing financial and logistics support. Therefore future C3 systems should aim to provide the interoperability and flexibility to integrate with other nations' systems.

3.1.5 Intelligence Product Sharing

Intelligence data is a critical element of Command and Control information. All nations closely protect the nature and deployment of intelligence collection assets, and this sensitivity feeds back into the releaseability of collected intelligence. This reluctance to share intelligence may adversely affect the conduct of multi-national operations. The challenge is largely procedural and may be met by sanisatisation policies and procedures – an important element of effective multi-national deployments.

The storage of data in a secure system is dependent on evaluation of risk factors which are a matter of national discretion. The evaluation processes themselves are usually sensitive issues and not published. But without an agreed evaluation process, there may not ‸ uniform levels of trust across C3 systems in a combined action. If one nation's system is not considered secure by a collaborating nation, then information sharing may be reduced to the lowest classification.

3.1.6 Fratricide Avoidance

Analysis of WWII and the Vietnam War show that on average 15% of all casualties in military conflict were inflicted by friendly fire. Such catastrophes were attributable primarily to errors in command and control. In the 1991 Gulf War 17% of Coalition casualties were by friendly fire. However, due to the relatively small number of Coalition ground casualties, the problem assumed a higher profile. To compound the situation, the press focused on facts such that of the 38 US armoured vehicles lost in the conflict, 30 were by friendly fire *(Reference 4)*. A key area in reducing the risk of fratricide is accurate and timely C3 systems.

3.1.7 Military Operations and the News Media

The combination of advanced technology and journalists keen to be at the front line, means future major conflicts will be fought under the unforgiving glare of global public television. The availability of suitcase-size satellite communications equipment capable of transmitting full broadcast-quality video from anywhere in the world gives journalists incredible power not only to report but also to shape events. Soldiers and journalists have shared a mutual distrust but in past conflicts have co-existed according to mutually accepted rules of conduct. However, gone are the days when journalists relied on military communications to file their stories from the front line. New technologies have effectively removed journalists' dependence on military commanders – hence the military have effectively lost control and censorship of the media. Gone too are the days when journalists' reports might have influenced only national feeling and strategic plans. Real-time reports now have a direct impact on immediate military plans.

The public's apparently insatiable thirst for accurate and real-time reporting, along with the falling costs of satellite technology, means there is every likelihood that major news corporations will acquire their own satellite reconnaissance assets in the near future. This would give the media the ability to look over the shoulders of the military anywhere in the world (*Reference 5*).

Real-time reporting by journalists is a rich source of intelligence for an attacking force. One example was the much-quoted event during the Gulf War when at precisely 3am on

January 17, CNN went off the air from Baghdad at the moment an F117 Stealth Fighter was due to deliver a bomb on the city's main communication centre. Arguably the first bomb damage assessment report of the war was filed by network television.

Real-time television is a powerful weapon in psychological warfare. In future conflicts, a military commander's actions must achieve a balance between countering the enemy and influencing public opinion. Traditionally this has been a lower priority area of command and control systems; however greater importance must be attached to this area of the *information war* if it is going to be exploited to the full.

3.1.8 Lessons Learned From the Gulf War

Many books and official reports have been written analysing the Gulf War, each drawing conclusions about the lessons learned. While many of these reports differ in their finer points, the majority agree that superior command and control was the key factor in the success of the Coalition forces. Other significant factors were superior technology (space, air power and precision-guided weaponry) and superior personnel. However, the Gulf War differed fundamentally from other conflicts and any lessons learned must be assessed cautiously when viewed in this context. There were a number of reasons for this difference: the principal ones being the time allowed for the Coalition forces to build up (6 months), the poor quality of the Iraqi leadership and the favourable (from an intelligence-collection view) desert environment. The Coalition's success hinged on using space assets for communications, navigation and intelligence. An analysis carried out after hostilities showed the Iraqis possessed jamming equipment capable of causing extensive disruption to these systems. It was unclear why the Iraqis chose not to interfere with the Coalition's space assets although this decision may have been influenced by the devastating demonstration of anti-radiation missiles in the early stages of the war. It is unlikely any future foe would be quite as co-operative.

3.1.8.1 Information Management

Many commentators considered the Gulf War to be the first *information war (Reference 5)* in that the outcome was driven by the Coalition's superior management of information. The conflict highlighted the benefits, and in some cases the disadvantages, of interconnected information systems. A key lesson learned was that information systems among air, land and sea combat units of all Coalition nations must be compatible if such units are to fight as a cohesive body. Further, both operational and administrative systems should be connected seamlessly. Many post action reports detailed occasions when useful information was denied to commanders because systems were incompatible.

3.1.8.2 Timely Intelligence

Another problem area identified by the conflict was the difficulty of analysing and disseminating intelligence, particularly at the tactical level, in a timely manner. The key source of intelligence in the Gulf War was technical sources, in particular imaging sensors. There are two major factors that must be considered. First, analysing imagery is essentially a manual and time-intensive task. The problem is encapsulated by the quote "satellite imagery is like viewing the battlefield through a straw". Post hostilities, many examples of poor Battle Damage Assessment (BDA) were reported by the popular press. Such stories included power stations and bridges being attacked by multiple air raids although in fact they had been disabled successfully on the first raid. Second, images are information-rich and require broad-band communications channels if they are to be handled efficiently. For example, a high resolution colour photograph can contain 20 MB of data. To pass this image over an audio channel, such as voice radio, would take 24 hours (assuming a standard 2.4 Kb/s data rate with 75% effective bandwidth without compression).

3.1.8.3 Communications Traffic Capacity

Insufficient communications traffic capacity was a problem which not only limited intelligence dissemination but also impacted adversely on general operations. The sheer volume of traffic was illustrated by the daily Air Tasking Order (ATO) which frequently exceeded 500 pages. In reality it peaked in late February 1991 when it was 982 pages detailing over 3000 sorties and had 175 addressees. The ATO was taking an average of 2.5 hours to reach Air Force Tactical centres, 3.5 hours to reach fixed communications centres outside the theatre of operations and 7 hours to reach other Service telecommunications centres. Even in this high technology war, the courier played a vital role – due to the inability of communications channels to carry the quantity of traffic. One modern twist, however, was that frequently the courier delivered a floppy disk.

3.2 Military R&D

3.2.1 The Changing Technological Environment

As the Gulf War demonstrated, the future battlefield will see a larger number of Precision Guided Munitions (PGM) which have a lethality many times greater than their added cost. However, the cost of acquiring delivery platforms is doubling with each new generation. For example, typical costs of operating advanced weapons (fighter aircraft and helicopters) are double the costs of the previous generation of weapons. Typically less than 20% of the cost of a modern warship is the hull and propulsion system. Acquiring and maintaining a minimum number of fighter aircraft and war ships is seriously stretching the budgets of the smaller and medium-sized ASEAN countries.

The end of the Cold War resulted in a surplus of sophisticated weapons available for sale on the illicit arms market. Using relatively freely available advanced technology, an unsophisticated foe can now develop or acquire extended-range missiles. For instance, during the Gulf War, Scud missiles deployed from mobile launchers required a disproportionately high technology solution and arguably the US-led Coalition never actually defeated the threat. Such weapons give a potential foe an enormous stand-off distance. The *1993 Strategic Review* also identified the possible proliferation of ballistic missiles as a key factor of change within the Asia-Pacific region.

3.2.2 ADF Directions

In November 1992 Dibb published a report titled *Strategic Priorities for Australian Defence Industry (Reference 6)*. The recommendations were broadly endorsed by the *1993 Strategic Review*. The report contended that R&D should be focused on areas which are key multipliers to our relatively small defence force. These are:

- Command and control, intelligence and integration of these areas;
- Surveillance and target acquisition;
- Adaptation of precision-guided munitions;
- Electronic counter measures
- OTHR improvements; and
- Satellite intelligence.

The report highlighted the last area by stating: "Australia's self reliant defence policy should move us towards less reliance on our allies for intelligence collection and surveillance capabilities in our own area of primary strategic interest." Later in the report Dibb recommended Australia should investigate light satellite technology with a view to acquisition of such nationally owned and controlled sensors before the end of the decade.

3.2.3 The Role of TTCP

The Technical Co-operation Program (TTCP) is an agreement between the five member nations (US, UK, Canada, Australia and New Zealand) to acquaint participating countries with each other's defence research. The agreement encompasses basic research, exploratory development and demonstrations of advanced technology developments. The agreement also covers exploration of alternatives and concepts prior to development of specific military systems. The aim of TTCP is to minimise duplication of defence research effort.

The activities of TTCP have changed significantly since the initial conception of the Program in 1957. Recent UN peace-keeping operations and the Gulf War highlighted the growing importance of multi-national operations. An essential element of these type of operations is effective C3 systems, which are tending to rely on advanced technology. International test bed activity, required to explore the potential and constraints of these advanced technologies, will be the key to progress of effective multi-national C3 systems. The aim is to achieve the goals of minimising the risk of fratricide and collateral damage in a multi-national operations. Ideally multi-national C3 systems would reduce the likelihood that firepower would have to used in a future crisis by assisting the rapid generation, analysis and selection of the best response options to adversarial situations.

The TTCP forum may also provide a basis for the traditional allies to explore, via test-bedding activity, technical issues arising from multi-national force operations with non-traditional allies.

3.2.4 Relationship with Industry

In the 1960s and 70s, the military R&D led the commercial sector in most fields of technology. However, the situation has now changed radically. First, the complexity of modern systems means there are extreme costs in developing them. Second, with economies of scale in the commercial market place, very complex systems can be produced and sold for relatively low unit cost. Hence there is a growing acceptance that the military should take maximum advantage of Commercial-Off-The-Shelf (COTS) products where possible. The principal advantage of using COTS products is high functionality at modest cost. C3 systems can unquestionably make extensive use of COTS because the military requirements are often very similar to products produced for commercial information systems.

However, there are negatives to using COTS products, the key areas being: lack of visibility of source code (and hence difficulty of interfacing and maintaining systems); keeping up with revisions (current software applications tend to be revised every 12 months); commercial users rarely *stress* applications to the same level as the military; and the frequently underestimated level of effort required to tailor COTS products to specific applications. An indirect problem also arises if the military is dependent on COTS – future military systems will themselves be shaped by what the commercial sector develops and makes available.

3.2.5 Co-operative Research Centres

Co-operative Research Centres (CRCs) were launched in Australia in 1990 as a government initiative to bring together academia, industry and other interested research bodies to research, develop, and commercialise advanced technologies. Selection for CRC status is by competition with an original government target of 50 centres in Australia. Currently there are 51 established centres and the program has now been expanded with a further 10 expected to be announced during this financial year. Funding is shared between all participants combined with an annual government grant.

DSTO is committed to CRCs as these are considered a key research multiplier. Examples of Centres to which DSTO is affiliated are: The Centre for Sensor Signal and Information Processing (CSSIP) with the University of South Australia; and the CRC for Distributed Systems Technology at the University of Queensland. Collaborative research with these Centres is expected to produce valuable C3 research products.

Selection for CRC status is competitive with over 50% of proposals being rejected. This has been in part due to the quality of applications particularly in relation to commercialisation potential. Also, of those CRC programs established, progress towards goals has been generally slower than planned. The main reason being that since project selection cannot be guaranteed, many of the proposed CRCs have a senior management structure comprising world-class researchers who invariably have committed calenders. Hence if successful, many of these key stakeholders have problems disconnecting themselves from prior commitments and becoming immediately fully involved in the CRC.

3.3 Standards

Adherence to standards benefits many stages of the system life cycle, including research, development, procurement, test and evaluation, training and maintenance. Generally, the benefits may be grouped into two areas: investment protection and technical flexibility.

Investment protection affects many C3 system aspects including: hardware, software, data, and training. Hardware standardisation simplifies logistics and can ensure compatibility of future applications with present machines. Software standardisation promotes modularity, scalability and portability of code. Together, these two factors contribute to network-wide sharing of limited, expensive resources. Data standardisation creates portable, transferable databases capable of being used simultaneously or independently by various applications throughout the echelons of a C3 system. Finally, with standardisation comes simplified training because users and maintainers can move more comfortably from one system to the next.

There are two types of standards: *formal* and *de facto*. Unlike formal standards, de facto standards are not recognised by an accredited standards organisation. Many industry standards are de facto at the present time due to the often lengthy review process required for adoption by formal standards bodies. The standards hierarchy includes three levels: Standards Organisations, Consortiums, and Vendors. The Standards Organisations are accredited and not-for-profit. Some of the major players existing at this level include: the Institute of Electrical and Electronics Engineers (IEEE), the American National Standards Institute (ANSI), the US National Institute of Standards and Technology (NIST), and the International Standards Organisation (ISO). This highest level primarily refines and adopts standards provided to them by the Consortia level. NIST is sanctioned by the US Federal Government, and their Federal Information Processing Standards (FIPS) are a primary source and direction for US DoD projects.

The Consortium level is populated by teams of academic institutions, corporations, and government agencies. These consortiums are usually specific to the standard(s) they wish to develop, and include groups such as UNIX International, X/Open, and the Open Software Foundation (OSF). Although their first priority is nominally development of standards for submission to the Standards Organisations, some consortiums operate as not-for-profit vendors of standards implementations. Most notable in this arena is OSF, with its Motif and OSF/1 (a POSIX-compliant operating system) products. At the bottom level of the standards hierarchy are the vendors who implement the ratified standards in their product offerings or incorporate the products of the consortiums within their own products as Value Added Resellers (VARs). It is from this pool of expertise that the standards initiatives usually spring.

3.3.1 Open System Interconnection

Arguably the most influential standard in the IT industry is the Open System Interconnection (OSI) reference model which is OSI standard 7498. This standard has delimited the processes and functions of interconnecting computer systems into seven main areas from the Application layer (what a user actually interacts with) through to the Physical layer (which specifies amongst other things electrical connections). Each layer represents a task or tasks necessary to get information from one application to another. Each level is concerned with the input from and output to its adjacent layer alone. Computers are thus compatible only up to the level that their OSI profiles are identical. The OSI model can be implemented by different organisations in different ways, as the standard defines only what the various levels should do, not how they should do it. The OSI standard covers many different types of applications, services and equipment and networks making selection of standards for specific application a technically complex task. To alleviate this problem, a number of organisations have developed functional profiles for specific systems. Essentially these profiles are a sub-set of options from the OSI suite of standards that an organisation mandates. Some nations have specified a Government OSI Profile (GOSIP) to aid procurement agencies. However, these profiles are a broad selection of base standards and do not assure interoperability. Alternatively, some International Standard Profiles (ISP) have been agreed which mandate a closely related set of standards which do ensure interoperability.

The lower OSI layers, Physical and Data communications standards are well established. However, there are likely to be some differences in the future as new systems try to improve on established technologies – for example new variants of Ethernet Local Area Network (LAN) standards are now being offered by vendors in an attempt to support multi-media more effectively.

At the middle layers which control networking, there are many de facto standards in competition with the OSI standards for example TCP/IP and Novell's IPX. Such propriety solutions offer more cost-effective functionality and are still growing in popularity. Sheer weight of numbers may eventually require that such solutions are adopted as OSI standards.

At the higher (application) layers there is growing market acceptance of some OSI standards – examples being X.400 for message-handling and X.500 for directory services. These series of standards are gaining some support for wide area and international/inter company messaging. However, while there is still pressure to adopt proprietary systems to provide local and within company electronic mail services, the non-proprietary Simple Mail Transfer Protocol (SMTP), has become one of the most popular electronic mail standards worldwide.

There are many problems for GOSIP and OSI in general. First, there is a misconception that OSI standards hold the key to the interoperability of C3 systems. C3 applications sit on top of the OSI model and hence are not covered by the OSI suite of standards. To compound the problem, no GOSIP has yet been defined for C3 systems and although the situation is slowly improving, it is generally recognised that the OSI standards do not address security issues adequately. Second, the US and UK Governments have specified GOSIPs but these are notably different from the Australian variant, particularly at the Networking layer. Finally, vendors have been generally slow at producing OSI-compliant application products and hence those that are available tend to be expensive and, as yet, have made little market penetration. A principal cost-driver has been the cost of validation and compliance testing. In the vacuum of OSI products, proprietary systems are gaining an increasing market share.

3.3.2 Open System Environment

OSI Standard 7498 is essentially a communications protocol which facilitates interconnection of heterogenous IT assets. However, a broader issue is standards to ensure applications can collaborate and interoperate. In June 1993, Cabinet endorsed AGGOS (Australian Government Guide to Open Systems) which offers guidelines to facilitate an Open System Environment (OSE). AGGOS is based on NIST's Application Portability Profile (APP). These documents give guidelines relating to the broader issues of collaborating and distributing operating systems, databases, graphics, user interface, programming environments and user interfaces. The goals of OSE are:

- Application portability;
- Systems and application interoperability;
- Protection of software investments; and
- Acquisitions from multiple sources.

3.3.3 POSIX

POSIX, which stands for Portable Operating System Interface for Computers, is a set of interfaces defined by the Institute of Electrical and Electronic Engineers (IEEE) in an attempt to achieve open systems. However, POSIX compliance has now become the lowest common denominator for UNIX systems and hence most vendors are claiming some degree of POSIX-compliance. POSIX is an example of a standard which has not progressed to meet market need and therefore is not being universally accepted. Consideration must be given also to C3 system developers applying POSIX, the concern being that a particular vendor's Operating System (OS), while it may be POSIX-compliant, may also offer services beyond those specified for POSIX. If the C3 system developer uses those additional features, the application may not be portable to another POSIX-compliant OS.

UNIX suppliers have been slow to make progress toward real open systems. Motif, COSE (Common Operating System Environment) and its first product CDE (Common Desk-top Environment) are probably the most significant events in this area and may form the model for future standardisation processes. The major players in the marketplace will come together and define a standard based on *best of breed* or some other compromise. They will publish some form of specification through X'Open or similar organisation and by common marketing will enforce the agreed standard on their customers. Smaller players will have to join in or get out of the market. However, there is a caveat to this principle in that it can degenerate into cheapest of breed. Suppliers might rush into the market with provisional offerings which have severe limitations. Procurement agencies tempted by the attractive prices might be buying long-term problems.

3.3.4 Desk-top Hardware and Software

In the 1980s IBM set the standard for desk-top machine with the IBM Personal Computer. The original PC was built round an 8 bit Intel chip and used a DOS operating system. Despite technical shortcoming caused by this architecture principally the ability to only directly address 1 Mega Byte of memory, 16 bit internal architecture and 8 bit external bus, the PC is still pervasive – particularly in the commercial sector.

The relative stability generated by the IBM PC is likely to be disrupted with emerging competition in desk-top hardware and operating systems – Intel 80x86 processors will be challenged seriously by RISC processors from IBM/Apple/Motorola – POWERPC, and Alpha processor from Digital – both consortiums are predicting shipping over a million units per year soon after product launches. Competition for operating systems will continue as users move from single-user systems such as DOS with Windows to multi-user successors such as Windows NT and Cairo, Apple moving to PowerOpen OS, IBM refining OS/2 into the Workplace OS.

Many consider what IBM did in the 1980s, Microsoft are doing in the 1990s. Microsoft has been accused of inventing its own standards and imposing them on the rest of the industry. To protect their market base, as well, Microsoft have made the commercial decision to limit information on their API standards and do not guarantee these standards in their products.

3.3.5 Software Development

The US DoD Standard 2167A is mandated for development of all operational systems procured by the Defence Organisation. It is essentially a document-driven standard and particularly for a large project generates copious volumes of documentation. There have been many criticisms levelled at the 2167A standard, for example, it leans heavily on other standards which must be understood before 2167A can be used effectively. The standard is all-embracing and needs tailoring to a specific projects need. Such tailoring is a complex task and generally organisations may not have personnel who are sufficiently experienced to perform it.

There is general shift of emphasis in procurement agencies away from documentation towards demonstrations. DoD-STD-2167A is designed principally for the classic waterfall procurement cycle and does not readily tailor to evolutionary-type procurement. Nor does this standard sit comfortably with non-hierarchical design methods, such as object-orientated methods. These criticisms have been addressed in an updated standard which will replace 2167A and two other related standards. The new merged standard, MIL-STD-498, will be published in 1994.

3.3.6 Future Standards

As new technologies become available and systems have become more complex, new standards will be required. Examples of such standards will be those addressing image transfers (currently covered by a plethora of options), digital map information, network management information, object management and high-bandwidth transmission systems (for instance ATM).

The related technologies are moving faster than the regulatory bodies can agree upon relevant formal standards. This means regulatory bodies can do little other than tidy up and rubber-stamp products which are in widespread use or are agreed to by all the major suppliers. As a consequence, users have little say in the process other than through their buying power. There is nothing intrinsically wrong with adopting and using de facto standards provided they are available in the public domain. Problems can arise when agencies commit to standards which are proprietary and so become locked to an individual vendor.

3.4 Security

Security encompasses a broad range of issues including the provision of resistance to battle damage, the prevention of unauthorised personnel from gaining access, and the maintenance of the trustworthy operation of communications-computer systems. A totally secure C3 system, if achievable, would be prohibitively expensive and most probably impractical to use. Therefore, the selection of appropriate security policies and mechanisms will require making a careful set of trade-off decisions – with cost being a major driver. Currently there are no effective cost/benefit analysis to assist procurement agencies in making these decisions.

3.4.1 Physical

As witnessed by the effectiveness of Precision-Guided Munitions during the recent Gulf War, physical hardening against todays' and tomorrows' threats is almost impossible. Distributed or alternative systems are the most viable options to achieve C3 systems with a high degree of physical survivability. The ever improving capabilities of our communications systems are beginning to provide the reliability and throughput necessary for implementing truly distributed C3 systems for most functional areas and echelons of Command and Control. At the same time, as our systems become more distributed and dispersed, the task of preventing unauthorised access becomes more and more difficult.

3.4.2 Communications-Computer Systems Security

Communications and computer security are playing an increasingly important role in the systems engineering process for our future C3 Systems. Our reliance on, and the security risks associated with automated information management systems (e.g. C3 Systems) continue to grow due to an explosion in the availability and sophistication of personal computers, workstations and networking. Communications and computer security are no longer the exclusive domain of the military, but are becoming increasingly important issues to commercial industry (e.g. banking, securities exchange, lotteries, airlines, etc.). As a result, we can expect to see more interest and activity in the development of secure commercial products and services and higher expectations from the users of our C3 systems.

In an effort to counter the threat of exploitation or denial of service, access to many military C3 systems is rigidly controlled and they are restricted to processing data of one security classification level. Unfortunately, due to the high cost of physical and personnel security, this *system-high* mode of operation is expensive to implement and maintain. It hampers the effective and efficient management of information, and it presents a significant barrier to achieving the configuration flexibility we so urgently need to support our diverse set of future military roles and missions. The costs of operating these systems must be reduced by eliminating *system-high* protection as the sole solution to responding to security requirements. Hence, there is a need for systems that are trusted to process information of various security classification levels simultaneously. This capability is referred to as Multi-Level Security (MLS).

3.4.3 Multi-Level Security (MLS)

An MLS system is one capable of controlling simultaneously access to data by users with different security clearances (and privileges) in a manner which ensures that users access data only for which they have appropriate clearance and need-to-know. (The term *system* includes the assembly of local and wide-area networks, hosts, workstations, applications software, etc.) MLS systems could provide senior commanders and their staffs with interoperable systems, a means to disseminate critical command and control and intelligence information, and to develop operational plans using a diverse set of computing systems operating at different security levels. The implementation of communications-computer systems that possess MLS attributes will ultimately rest on the ability to:

- Develop and document security policies;
- Implement mechanisms to enforce those security policies;
- Verify the correct operation of products and systems; and
- Develop standard certification processes that are accepted across and between our national military authorities.

3.5 Procurement Issues

Acquisition of any military materiel, including C3 systems, cannot be divorced from procurement realities. Therefore for completeness a brief overview of significant procurement issues is given below.

3.5.1 User Expectations

The last two decades have seen an explosion of IT products change the way business is done across virtually every aspect of normal living. The coming generation of senior military officers has grown up with these IT-driven changes and hence has a greater awareness of computers than hitherto. This generation of users will be computer-literate and as a consequence perhaps more questioning and demanding of technology.

Gone are the days when keyboard skills solely resided in the typing pool. The coming generation of military decision makers are likely to be keyboard-literate. This generation of users will be accustomed also to tailoring software applications to meet their own individual requirements. This tailoring includes not only changing the screen interface details such as colours, fonts and sizes but also the generation of macros to simplify tasks and to do tasks more effectively. Such conveniences are widely available on domestic and office-type systems and will be expected by users of future C3 systems. Allowing the user to generate high level code or macros is often referred to as accommodating *user developed software.*

3.5.2 User Involvement

It is generally accepted that involving the military user in acquisition project teams is a positive step. The benefits include the end-product tending to closer meet the military requirement and a greater sense of ownership and therefore acceptance of any new system. However there are two notable caveats to this process. First, the military posting cycle. The rotation of key personnel every two years can be extremely disruptive to a long term project. Second, the military reporting system. This tends to report on quantifiable achievements whilst in post. This could place the military user in the dilemma of deciding between directing energies towards short term objectives or longer term project goals.

3.5.3 Evolutionary Acquisition (EA)

The Defence approval processes is based on the classical Waterfall (so called because of the serial nature of activities) procurement strategy. This is a mature project management technique which has been taught for over 20 years and occupies a salient position in management training. In the past, organisations have considered it a safe, logical, systematic method of project management. The classical technique is based on analysing the market need, specifying the requirement, evaluating design options, and implementing and supporting the favoured option. However, there are three problems with this technique, it assumes:

- You can write a specification for the total requirement at the beginning of the project cycle;
- The requirement remains stable during the implementation; and
- The system can be modelled using structured analysis techniques.

However, for C3 systems it is now acknowledged that it is impossible to specify all the user requirements up front. Many requirements for C3 systems can be derived only from the experience of actually using a system. Technology is also advancing at an ever-increasing speed. Hence, more advanced products are becoming available which could enable C3 tasks to be completed more efficiently and effectively. Moreover, the threat is continually evolving. As a consequence, for C3 systems a change in requirements will be the rule rather than the exception. A further key fact is that C3 systems have an intrinsic structural complexity that makes structured analysis techniques inappropriate.

Therefore, there is growing acknowledgment that procurement strategies based on the Waterfall methodology are inappropriate for C3 Systems. Experience amongst the nations demonstrates that such methods are in part responsible for projects being over budget, behind schedule and obsolete on installation. As a consequence, the delivered systems have often generated much user-dissatisfaction. An alternative approach is the new and emerging procurement strategy called Evolutionary Acquisition (EA) in which systems are developed incrementally. In EA, a core or baseline capability and subsequent increments are procured as distinct projects for which risk can be kept to an acceptable level. Therefore, a correctly-managed EA can reduce significantly a project's exposure to cost, schedule and technical risks. The main advantage of EA is that it provides a method to adapt systems to changing user requirements in a cost-effective and timely manner. Initial experience from US military and civilian environments has validated the underlying principles of the concept.

EA conflicts with the current Defence approval processes on many counts. The main problem lies in that all-up project costs cannot be identified at the time of project initiation. The timing for traditional approvals is based on the annual national buuget cycles, the governing regulations of which are enshrined in the Constitution and Common Law. EA increments would require approvals much more frequently.

ADFDIS (Australian Defence Force Distributed Intelligence System) and JP2030 (Joint Command Support Environment) are major projects that are in the early stages of procurement. Both of these projects are embracing many of the principles of EA.

3.5.4 COTS

There is an overwhelming economic case for Defence to make maximum use of COTS products. However this strategy introduces a new aspect to the life-cycle suppon for hardware and software.

Defence produced compilers, software applications and tools were costly but assured availability of support for a 20 year lifetime. In moving to COTS software, the best leverage that defence has in obtaining the support required is to procure in large buys in order to obtain the attention of the vendors. Even old software will continue to be supported as long as a profitable market, based on a high original volume of purchase, exists. However, it is unlikely that the Australian defence market is large enough in global terms to achieve this goal. An alternative strategy is to maintain an Applications Programming Interface (API) that allows defence developed software to be ported to new compilers and operating systems with ease. This means using mainstream COTS products to begin with. There is little doubt that UNIX, C and C++ support will be available for a long time, but the future of Ada, outside mission critical embedded systems, is a little more uncertain.

As fault tolerance and mean-time between failure of hardware begin to meet complete deployment times, we will be able to eliminate or curtail severely requirements for other than depot-level maintenance. We have seen such technology advancement in the computer industry in that a three-year-old computer is thrown away because the annual maintenance cost exceeds the cost to buy the latest model. As computing and communications technology continues to advance, obsolescence of defence systems will accelerate.

3.5.5 Program Management and Budgeting

The ground stones for Program Management and Budgeting (PMB) were layed in April 1984 when the Government published a policy paper titled *Budget Reform*. In this paper were two complementary reforms namely the Financial Management Improvement Plan

(FMIP) which aimed to streamline the budget process and PMB which was designed to focus attention on setting objectives and measuring performance against these objectives. Under PMB, allocation of funds was no longer completed by a system of votes (parcels of money for specific kinds of spending) but by funds allocated to program managers and their subordinate managers. The principal intentions of PMB were to reorganise defence activities onto a more commercial-orientated approach and increase the job satisfaction of defence managers by devolving management of funds to the lowest practical level within the organisation. PMB was formally introduced into service on 1 July 1990.

PMB is intended to devolve financial control to the lowest practical level. If financial control for a project was given to the Project Director, this could have a significant impact on the acquisition process. It would give the Project Director greater control and flexibility in directing the outcome of the project. PMB and EA are complimentary initiatives which are ideally placed to support acquisition of C3 systems which are allowed to evolve to meet dynamic user requirements.

3.5.6 Commercial Support Program

In 1990 Wrigley published a report titled *The Defence Force and the Community* which identified considerable (almost $400 million a year later revised to $350 million) scope for industry support of the ADF in the areas of contracting out and commercialisation. The 1991 Force Structure Review stated that contracting out support functions would release resources and funding to make the combat potential of the ADF more effective. The report made the distinction between core combat and combat-related functions on the one hand and support functions such as catering, stores and transport, administrative support, non-military training, repair/maintenance, communications, medical and fire-fighting (non core) which it recommended should be contracted out. The Commercial Support Program (CSP) is being implemented in 3 phases (tiers) and is currently completing the second tier.

The major impact of CSP on C3 systems will be in the area of communications. Civil communications carriers in Australia have over $26 billion of infrastructure. There is a strong economic case that the military make maximum use of this national asset and has been directed to do so (*Reference 8*). This could involve not only the use of civil communications infrastructure but also technical expertise in operating and maintaining communications systems.

3.5.7 The Defence Budget

The ADF is not immune from the near global defence budgets reductions, although perhaps understandably, since the Australian security environment has changed relatively little since the end of the Cold War, cuts were less than in other Western nations. In Australia no real economic growth in defence spending is forecast for the rest of the decade. Financial Year (FY) 1993/94 saw a 0.75% reduction in real terms with a further

0.5% reduction scheduled for this financial year. The Defence budget for FY 1993/94 was $9,786 million which was 8.5% of Commonwealth outlays and 2.3% of the Gross Domestic Product.

C3 systems are recognised as an essential element of effective military operations and are generally considered a force multiplier. Although the overall Defence budget is falling in real terms, it is however likely that spending on C3 systems in the medium term will increase.

SECTION 4
VISION OF FUTURE C3 SYSTEMS

4.1 Key Elements of Future Systems

To facilitate analysis of visionary C3 system a series of seven sub systems are considered with eight functional requirements. From a theoretical viewpoint the following classification is clumsy since it tends to mix function and technology and generally fails to recognise the interconnections and complexities within a C3 system. However, for clarity the following breakdown is used since it is in line with current C3 models.

4.1.1 C3 Sub-systems

4.1.1.1 Situation Display/Data Fusion

This is the functioning heart of any C3 system. In the earliest days of major conflicts this may have been as simple as the General setting his command post on a good vantage point of the battlefield and communicating with his subordinate commanders by messenger or flags. In modern times the concept has changed little except that the battlefield may be continental or global in scale; the sensors have extended the range of the General's eyes and ears and the whole system is supported by communications systems which can convey greater volumes of information.

The main aim of the situation display sub-system is to establish location, identification and intention. To achieve this aim there is a need to fuse information from multiple sources. But often this information will be incomplete and uncertain. The system would show own forces, friendly forces, neutral, potentially hostile and hostile forces. It would have the ability to display relevant civilian aspects such as merchant ships, civil aircraft, and population centres. The sheer volume of information required dictates the system should depend on automatic input of information via communications in some way or direct input of information from databases on other systems. To support joint operations the situation awareness systems would be able to show not only the land situation but also the sub-surface, air and space picture. The space element would show positions and capabilities of satellites, projected orbits and footprints.

The most important requirement is that the situation awareness system must present a common picture which is available at all levels in the hierarchy and, if multi-national forces are involved, across service and national boundaries. It need not be the same actual system. It may be built on different map systems and provide different analysis tools but situational information must be the same. The common picture would help avoid fratricide and also encourage greater effectiveness through synergistic initiatives if all forces taking part in an action can see overall objectives.

A key element of the modern situation display is a Geographic Information System (GIS). The system would also be able to accept overlays, for example overhead imagery and weather charts. The GIS would be required to provide varying levels of map/chart detail. At the higher levels of C3, country outlines may be sufficient. For the tactical level, highly accurate 3D data may be required and the sub system would have to be capable of spatial reasoning, for example whether point A is visible from point B given the contours, terrain covering and weather?

A problem that would have to be resolved is management of the quantity of information given to a user, to avoid overload. The system would start by allowing access to a minimum of data and then focus on detail as required by a user. Hard-wiring a system to deny a user information detail is inappropriate since a user must able to *drill down* to find key information when required.

The situation display should be an integrating platform on which other planning aids may be built. To achieve this the system would have to have a time dimension, that is, it would be able to replay a situation as it was, and be able to show plans and anticipated movements. In this way a commander could explore *what if* simulations in formulating future plans. The system would be able to support conference sessions with multiple users sharing a common picture and be able to discuss situation and planned actions.

The situation display would be used to assist in preparing briefs. Thus it would be integrated with other tools, and enable cutting and pasting from maps to other screens or documents.

For all its complexity, the situation display module must be intuitive and easy to use so that operators need little or no training.

To exploit the mind's ability to recognise patterns and deduce trends, virtual reality and battlefield simulation are a natural combination for the situation awareness system of the future. Commanders will be able to *fly* over a battlefield viewing their sensors' perception of enemy units and formations. This may reveal a better understanding of the enemy's intentions. They will also be able to see what their own forces look like from an enemy perspective.

4.1.1.2 Message Handling System

The Message Handling System (MHS) as a separate system will disappear gradually from future systems and will merge with e-mail and office automation type products. The transport and transmission of messages will use data communication standards rather than old telegraph standards. All future MHSs will use general purpose hardware and tailored COTS software. To permit global use, standardised directory services (e.g. X.500) are essential.

Future COTS applications will integrate seamlessly with e-mail so that it will be as much of an option to transmit the document as to save it locally. Future e-mail systems will support transmission of compound documents which contain embedded objects such as spreadsheets, image, audio and video-clips.

At the tactical level, it is likely there will always be limitations in communication bandwidth. Therefore there will be a need for intelligent gateways which can provide a subset of these full capabilities to the tactical commander.

4.1.1.3 Decision Aids

Traditionally, automated decisions aids have operated in isolation from their working environment. For example, optimisation techniques have required that all values are entered before the program runs. The program then takes some time to calculate its answer. This approach is fine for very stable domains. However, most problems are solved in dynamic and uncertain domains where information is missing or may be changing constantly. Future decision aids and problem solving support will recognise that problem definition and task performance are both situation dependent. Therefore future problem solving tools will constantly sense their environment to determine if they are still solving a relevant problem using the most suitable task available.

Decision aids, like people, have to acquire knowledge in their operating environment. Traditionally this has been done through people laboriously entering more knowledge they thought was relevant. Knowledge acquisition in the future will be done through learning. Current machine learning techniques are in their infancy. Future systems will learn from situations and be able to suggest how to perform a process more efficiently.

4.1.1.4 Text Management

The Text Management system will be an integral part of future C3 systems. Intelligent systems will build profiles and filter systems for individual users dependent on the actual scenario and the user's personal requirements. Intelligent agents will then search and monitor for relevant information through multiple networks and databases. Sources would include Australian and allied: wire services; electronic newspapers; CD-ROM publications; library services; commercial databases; and intelligence repositories.

Registry systems will be integrated into office automation products and capture all printed correspondence which enters or leaves a C3 system. In addition the system could capture all voice communication by applications of speech recognition and converting the conversations to text. Intelligent searches could then be carried out on the registry.

4.1.1.5 Resource Databases

It is impossible to have instant access to all the information necessary to conduct all possible operations. The exact information requirements will be impossible to define in advance for an operation as requirements will be scenario-dependent. Thus information will be extracted or *pulled* from databases maintained by other systems, e.g. logistics, personnel and intelligence. Having built the required databases for a specific mission, there would then be a requirement for automatic update. As well, should the information be critical to the mission, replicas would be generated to improve survivability. Resource databases would not have stand-alone user-interfaces but would be integrated fully with situation awareness and OA systems.

Future resource databases will be able to find what information is available in linked databases by direct examination of the database's internal arrangement or schema. Future network management systems will make such schemas available across networks.

4.1.1.6 Video and High Resolution Colour Graphics Imaging

Humans can process visual data faster and easier than any other form of stimuli. Visual data has a type of fingerprint that the human mind clearly retains many times better than text alone. Human eyes have the highest bandwidth of any of the human senses. The eyes are estimated to be 80 times better at collecting and processing information than the ears. Hence future C3 must exploit this by making maximum use of video and imagery.

Video Teleconferencing and high resolution imagery will revolutionise C3 systems in the next decade. Video in this context is used to cover a broad range of activities examples being video conferencing, electronic collaborative whiteboards, promulgation of briefs, real-time surveillance of the area of interest and news feeds such as CNN. For example, use of high resolution imagery would be used for surveillance, targeting, battle damage assessment and telemedicine. A technical challenge for imagery will be that of obtaining screen resolutions equivalent to photograph/printed images.

In the far future, on-line digital manipulation of the video/image will merge into 3D representations and virtual reality systems.

4.1.1.7 Network Management and Information Flow Control

C3 systems of the future will have greater connectivity to local and wide area networks. A major problem will be the administration and maintenance of these networks. Networks of the future will have embedded intelligence to self optimise and self heal in case of damage.

A significant challenge for future C3 systems is preventing information overload of users. Whereas the processing ability of hardware may match the information explosion in the world, the limiting factors will be communication links and more importantly, the human in the loop. Tools will be required which can monitor, analyse, prioritise and control the flow information in C3 systems, if they are to avoid information saturation.

4.1.2 Functional Requirements

4.1.2.1 Security

Future C3 systems will be able to support processing information ranging in security classification from Unclassified to Top Secret. The system will be partitioned with areas restricted to a limited sub-set of classifications. Users will identify themselves at each terminal via a biometric-sensor, for example retina pattern matching, and will be able to operate only up to their authorised security level. Trusted gateways will monitor all traffic, be it text, image, data or video leaving a higher classified system to a lower system.

4.1.2.2 Survivability

Future systems will be designed with no single point of failure, full redundancy of data and communications channels. If one part of the system is disconnected, the remainder of the system would be able to recover automatically. From a user perspective no operation or information would be lost in any conceivable fault condition.

4.1.2.3 Flexibility

The functionality required of a C3 system is scenario-dependent. Future C3 systems should be highly flexible, and able to be configured, at short notice, to meet a specific mission.

4.1.2.4 Portability

Future systems should not be dependent on any single vendor for software or hardware. This will enhance robustness in the C3 system to vagaries arising from commercial pressures and reduce this dependence that needs to be placed on individual suppliers of hardware and software.

4.1.2.5 Scalability

An ideal system would be able to be expanded incrementally without major hardware or software implications. These updates could be implemented without any deterioration of system performance.

4.1.2.6 Interoperability

Interoperability will be achieved by common communications standards and agreed data exchange standards. This approach will permit different services, agencies and other nations to operate their own preferred applications while being able to share data seamlessly and hence to interoperate.

4.1.2.7 Useability

Users can look forward to systems which require minimal training which are adept to use and which have interfaces and functions designed to maximise their effectiveness for individuals and teams.

4.1.2.8 Transportability/Mobility

Support to the Commander on the Move will continue to be as vital as the commander's physical presence within the area of operations. Advances in the relevant technologies will enable the vision of a virtual deployable command centre to be realised. This will mean that specialist staff support, advice and information processing capabilities provided by an operational command centre will become increasingly available on call regardless of the commander's actual physical location. Vehicle-borne facilities appropriate to the C3 support required by the commander on the move are being improved continually to offer richer and more efficient capabilities within the communications bandwidth-constraints that apply at the time.

4.2 Future Architectures

In order to emphasise command support system capabilities rather than information system implementation requirements, future architectures will clearly distinguish the two. Separating command support system issues from information system implementation issues focuses attention on the business a CSS is supporting. Hence future architectures will show CSS framework being supported by the Information System.

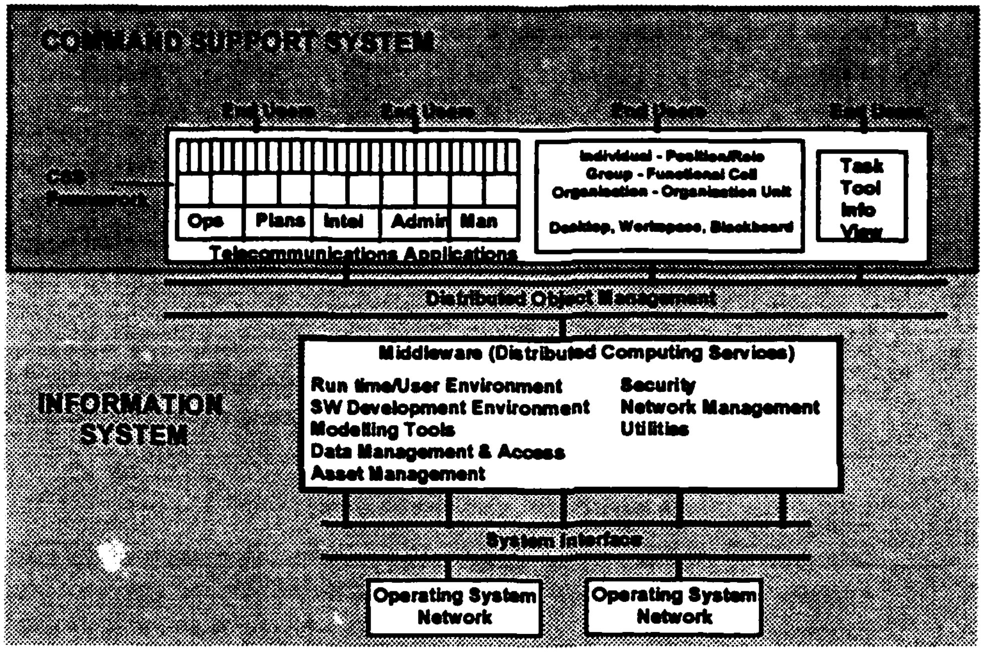

Figure 1. Open systems architecture for object-based application development

4.2.1 Information System Issues

Standards for distributed information systems are emerging which will enable object-based applications to be constructed and maintained across heterogenous computing environments. Distributed computing services and object-based applications are encouraged because they have the potential to increase re-use of components, interoperability and portability. Services which are common to applications and sit between the application and the operating system are known as *middleware*. The aim of middleware is to provide a high level, platform-independent environment for the development, maintenance, and run time support of distributed applications (see Figure 2).

Middleware will provide many of building blocks for the development of heterogenous, autonomous, and distributed systems. Among the distributed computing services provided by middleware will be: user interface components, a distributed computing environment, a software development environment for computer-aided software engineering, modelling tools, data management and access, asset management, computer network management, telecommunications, network management, and security.

The Open Software Foundation's Distributed Computing Environment (OSF's DCE) is a standard which is forming the backbone to many middleware products. DCE permits applications to be constructed which can access processes and information running on a number of different platforms. Remote procedures calls, distributed file systems, portable threads and distributed time services provide cross platform interoperability. OSF's Distributed Management Environment is designed to provide network management, application and user interface (Motif) services.

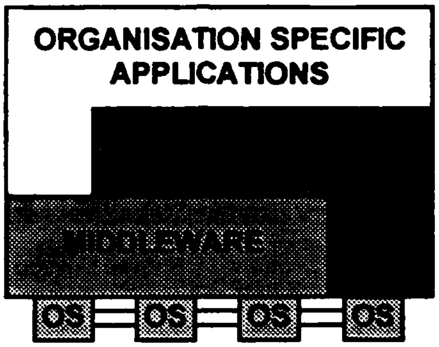

Figure 2. Application construction and maintenance services for interoperable ISs (OS = operating system, CORBA = Common Object Request Broker Architecture).

Development of applications on top of middleware services will require an architecture which allows distributed application integration. Object-oriented architectures such as the Object Management Group's Object Management Architecture (OMG's OMA) has been designed to enable the integration of distributed object-based applications. OMA seeks to achieve object distribution transparency, extensible and dynamic implementation of objects, discretionary access to objects, notification of events to interested objects and support for inter-object semantic relationships. OMG-compliant technologies are beginning to emerge such as the Common Object Request Broker Architecture (CORBA) which provides mechanisms for objects to make requests and receive responses transparently. CORBA requires an object model which permits distributed object management. However, there is no single object model. This is because applications and domains have different requirements. To overcome these problems, OMG has adopted a Profile approach which specifies a core object model plus domain-specific components.

4.2.2 Command Support System Issues

It is now well recognised that the user requirement for CSSs is unlikely to ever be static and will evolve. User requirements change because they depend upon what the situation is and the style, personal preferences and experience of the individual commander. They also depend upon a technology base which is changing constantly.

Support for the core business of command and control such as applications for operations, planning, intelligence, administration and management will be developed using an object management system. Each business application will then be specialised for activity segments such as air surveillance or maritime interdiction. Local specialisations will be for specific organisational units. The development of these applications should occur in a command support system business framework. The framework would provide an explicit representation of the business of command and control, and enable users to tailor the services provided by the system to meet their requirements.

Object-oriented mechanisms have the potential to provide a dynamic and extensible environment. Users will be able to access information and to construct objects that are meaningful in their domain. The user may know nothing about how or where the objects are stored. The user will be able to state how they would view the objects, for example, as a document, as a table, or a graph. The same object could thus have several views. Mechanisms will also be implemented allowing association of views of different objects for specific roles to achieve a purpose.

4.2.3 Summary

Specifying the requirements of C3 system that is at the individual, group or organisation level, for the entirety of the system's life is impossible. The individuals, groups, and organisations will all change with time. The situations and the environment will also change. The solution to this problem rests in the development of a support environment which is specified and tailored by users and which can accommodate change over time. An architecture which achieves this aim is illustrated in Figure 1.

The key technologies underlying the architecture are middleware and distributed object management. However, these technologies are designed principally for the professional software developer. A CSS framework is required if end user change is to be achieved.

It is likely future architectures for C3 system will support evolutionary development. The basic information infrastructure will be provided by the procurement agency. However, the functionality of the CSS will be flexible and the decision of the organisation and the user.

4.3 C4I for the Warrior

There are numerous places in this section where information is presented from the US Office Of the Joint Chiefs of Staff *C4I for the Warrior (Reference 7).*

The WARRIOR concept is an ambitious goal Command and Control, Communications, Computer and Intelligence (C4I) system architecture for the US military. It has its origins in lessons learned from the 1991 Gulf War and aims to realise a fully-integrated global command and control system for joint interoperability of all US military. A Warrior is the man or woman who fights the war, whether from a foxhole or from a Commander-in-Chief's command post. The C4I for the Warrior concept provides a beacon that will guide all Services to a global C4I system which satisfies the total information requirements of Warriors when they fight as a team with a common mission. The global vision of C4I for the Warrior is to create for these joint war fighters a single view of military C4I. This view is a widely distributed, user-driven network to which the Warrior *plugs-in.* This network provides:

- Seamless, secure connectivity;
- Multiple, highly flexible nodes;
- Access to all other operational elements and databases (which are automatically updated and from which desired information can be pulled); and
- All the required information for any assigned mission.

The increasing complexity of multiple force operations in modern warfare is new as are the C4I tools and processes available and needed to plan, co-ordinate, and carry out these tasks. The concept of teamwork is not new. The fighting force that over-ran Iraqi defences validated again the long-standing military axiom that victories are gained by close and effective integration of ground, sea, air and amphibious resources. The C4I for the Warrior concept facilitates teamwork, turning a vision of a fully integrated C4I support system into reality.

The need for interoperability among Services and nations is well known and is a generally accepted premise. The term interoperability has little meaning unless specific parameters are described and specified. Interoperability encompasses doctrine, procedures and training as well as systems and equipments. In the C4I for the Warrior concept, interoperability is the capability of people, organisations, and equipment to operate effectively together so that "every unit on the battlefield can share information with every other unit on the battlefield."

The Joint Staff will co-ordinate with the CINCs (Commander-In-Chief), Services, and Agencies in a phased, team approach, which will provide the flexibility to absorb the dramatic changes which technology, budgets, and politics may impose. The approach:

- Capitalises on the current investment in C4I systems;
- Provides for the capture of new technology;
- Minimises disruption to ongoing programs;
- Focuses from the start on the adoption and use of common information exchange standards to achieve interoperability among existing as well as future systems; and
- Demonstrates full compliance with policy guidance and direction.

There are three phases to the Plan:

- Quick-fix Phase, current ;
- Mid-Term Phase, expected to last 10 Years; and
- Objective Phase, to commence on completion of Mid-Term Phase.

The initial phase addresses quick-fixes to service and agency-independent stove-pipe and manual systems. The objective of the quick-fix phase is to take actions now that will result in near-term interoperability improvements. Quick-fixes include the installation of translation devices that interpret non-standard message and data formats and protocols and produce common outputs that can be readily exchanged via standard transmission. All unique systems that require manual interfaces or elaborate buffer-translator processes to establish interoperability are identified and modified. Eventually they will be eliminated as unique systems evolve. All architectures will be analysed for interoperability and commonality resolutions. Joint and combined C4I policy, doctrine procedures, and programs coalesce into one co-ordinated approach. The Mid-Term Phase produces a global C4I system capable of generating and delivering the fused information needed for tactical command decisions. The Mid-Term Phase is concurrent with the Quick-fix Phase and encompasses the Program Objective Memorandum (POM) period plus the following ten years. During this phase:

- Interoperability becomes fully integrated into the policy, doctrine, and systems acquisition processes for all new C4I systems and modernisation programs;
- Modular building blocks are described in technical detail;
- A common network operating environment cements the modular building blocks into a joint network;
- Applications interoperability and standardisation produce fixed, transportable, and tactical communications and information nodes that are interconnected in support of joint or combined operations irrespective of time, place, or Service Agency sponsorship;

- The joint global C4I infrastructure evolve: toward a single common, unified interoperable system; and

- Migration from unique military standards to commercial national and international standards.

The objective phase extends beyond the year 2000 and is very dependent upon advanced technology drivers. The concept description itself should provide the focus needed by the research, development, and acquisition communities to generate solutions. It is unconstrained by nostalgia and free of the design predicability that prematurely dismisses relevant options. Necessary progress is expected in at least the following areas:

- Artificial intelligence applications;

- Multi-Level Security;

- Data compression and data fusion;

- Common operating and interface environments; and

- Common display unit technology is capable of producing a common, integrated, multi-media, multi-functional display terminal. The terminal provides colour graphics display battle element and geographic icons, overlaid on all or selected portion of the Warriors battle space display; embedded features include data-link encryption, secure voice and video transmission, and decision-aiding/targeting support applications.

4.4 ADF C3 System Directions

The ADF Command & Control Information Systems Plan (ADFCCISP), currently in draft, proposes the future direction for Australian C3 systems. The Plan addresses strategic, operational and tactical level C3 systems that are in service, in development and planned up to the year 2000. The plan embraces many of the features of the C4I for the Warrior as reinforced by the Plan's opening quote taken from General Colin Powell US Joint Chief of Staff:

> "The ultimate goal is simple: give the battlefield commander access to all the information needed to win the war. Give it to him where he wants it, when he wants it and how he wants it".

The purpose of the ADFCCISP is to define the functions and interaction of all C3 systems supporting the command and control of the ADF. The Plan aims to coordinate and control the development of C3 systems to avoid ad hoc developments, minimise duplication of effort and ensure interoperability. Specific aims of the plan are to:

- Specify the Command and Control Information Systems (CCIS) which are required to manage the Operational Information (OI) and fusion processes identified in the ADF Operational Information Master Plan (OIMP);
- Allocate responsibilities for developing these systems;
- Describe the overall goal CCIS environment, architectures and interoperability requirements based on the current command and control structure, policies and doctrines contained in the ADFP1 (ADF Publication 1 titled "Doctrine");
- Specify the interfaces which are to exist between the ADF CCISs: and
- Specify the major types of OI and formats that will flow along the interfaces.

The ADFCCISP is scheduled for publication late 1994.

SECTION 5
TRENDS IN C3 SYSTEMS TECHNOLOGIES

The pervasive nature of C3 systems means that there are a very wide range of supporting technologies which must be considered. The issue is complicated because as yet there is no universally agreed reference model for C3 systems. Hence classification and sub-division of related technologies is not straightforward.

The approach adopted for this report is first to give a high-level appraisal of Systems Engineering issues (Section 5.1). This represents a wide range of technologies. In addition to the traditional approach of including Hardware and Software Engineering issues under this heading, additional topics covered are Information/Knowledge Engineering and Human Engineering. The first of these topics is included in recognition that the primary attribute of a C3 system is the information and knowledge which it harnesses. Human Engineering is included because in the next 15 plus years the human operator will remain an integral part of any strategic and operational level C3 system. Section 5.2 *Enabling Applications and Tools* is a lower level description of specific technologies pertinent to future C3 systems. Section 5.3 *Communications* is a sub-section in its own right discussing main directions and support to the Mobile Commander. While recognising that sensors and intelligence sub-systems unquestionably are an integral part of a C3 system, this report covers only sensors which will have a major impact on Australian future C3 systems (Section 5.4).

This report is tailored for non-technical C3 system specialists and hence the depth of coverage for each topic is limited. A capsule summary of each topic is given.

5.1 System Engineering Issues

5.1.1 General

5.1.1.1 User Requirements

User requirements identification and specification are recognised as a critical phase of a system's life cycle, where the seeds of project success or failure are most frequently sown. This is particularly the case for C3 projects, where the functionality is complex, multi-faceted and, in some cases, unique. There now exist a number of comprehensive methods and tools, some of which are mandated for government projects. Unfortunately, these are not proof against failure. Indeed, one of the major difficulties of establishing and specifying requirements is concerned more with the acquisition process than methods and tools. User Requirements definition for a 'Big Bang' procurement is far harder and riskier than the same definition under an Evolutionary Acquisition procurement.

Given the move towards Evolutionary Acquisition (EA) for C3 procurements, an important trend for user requirements formats, methods and tools is to provide a better *fit* with EA practices. Some specific aspects are as follows:

- Specification formats tailored for EA (overview of system, architecture, core system and so on);
- Use of prototypes in parallel with specifications (see also prototype section); and
- Integration of requirements with COTS product capabilities (implying a closer integration of requirements, design and coding).

5.1.1.2 Prototyping

For more than a decade, conventional methods of software development have followed the waterfall model (grand design or big-bang approach). Nowadays, although they provide a systematic approach to software development, conventional approaches are severely criticised, in particular for the development of large-scale Information Systems (IS). Excessive slippage in implementation schedules, unacceptable cost over-runs and unfulfilled requirements are commonly reported. The principal reasons for the project failures are the following: the methodologies used are not appropriate when requirements are not well understood; the paper representation of the requirements means that the system remains abstract for the user until it is implemented in the final stages of the project; and the acquisition process is too long, too slow and does not allow for an efficient system growth and easy integration of new technology.

Prototyping approaches offer an attractive solution to these problems, as they involve the users throughout the full life cycle of the system and as they rapidly exhibit the essential features of the operational system. The broad meaning of the term *prototyping* and the fact that it has been associated for a long time with a bread-board approach has created much confusion. To solve this problem, NATO has provided common definitions. Three broad classes of prototyping are identified, depending on the goal to be achieved:

- *Exploratory prototyping*. Used to clarify, by means of simulators or testbeds, user requirements and desirable features of the target system. Alternative solutions, perhaps a basis for experimental and evolutionary prototyping activities to follow, may also be discussed.
- *Experimental prototyping*. Used to test, using testbeds or prototypes, the validity and feasibility of proposed design decisions before investing in large scale implementation of the target system.
- *Evolutionary prototyping*. Used where a prototype is developed and evolved through a number of versions, (beyond a testbed) until it is considered to be adequate to meet the users' needs with the aim of eventually obtaining acceptance as an element of the final operational system.

Prototyping is seen as one of the prime means of establishing requirements for novel features or functionality. A prototype itself can range from a few *storyboards* to a fully functioning sub-system, depending on its function or goal. There are a large number of prototyping tools available, ranging from User Interface Management Systems (UIMS) to macro-languages within COTS products. The choice of tool is an important factor in ultimate success. As COTS packages become more powerful and easier to tailor, they offer the opportunity for C3 prototypes to be delivered to the user as robust and flexible systems for trial. This trend is likely to continue. Specific issues which are being addressed include:

- Integration of prototyping environments with target environments, with openness in terms of Operating Systems, Graphical User Interfaces (GUI) and programming languages;
- Integration of prototypes with formal specifications;
- Integration of specialist prototype environments with COTS products; and
- Auto-code generation (particularly with 4GL and 5GL).

5.1.1.3 War Gaming

War-gaming has no universally agreed definition but is generally taken to cover a broad spectrum of activities from field exercises such as the Kangaroo Exercises through to fully automated simulation of military conflicts. As a general rule simulation tends to focus on the doing phase of conflicts and ignores the planning phases. Other examples of war-gaming include military planning games played out in a seminar environment, and command and control training exercises using operational systems.

A key ingredient of war-gaming is an opposition. The opposition may be *canned* that is tightly controlled to give a predictable result or be adaptive and have intelligence. The adaptive option normally requires human operators in the system.

For effective training, simulation must be believed valid by commanders and staff. If a model is not credible to its users, they will attribute negative results due to deficiencies of the model and ignore them. To encourage the commitment of exercise participants, the realism of the enemy is extremely important. Political sensitivities often preclude the use of real neighbouring countries and hence fictitious foes are frequently created and used. However, often an unrealistically low amount of information is created about the fictitious foe and this can lead to dissatisfaction among exercise participants.

Another important feature of war gaming is that the passage of time can be controlled by the exercise administrator, that is, time can be compressed, stretched, frozen, re-run, reflect reality or a combination of these options.

Arguably the best value training for commanders and their staff is to train on C3 systems that they would use in a real situation. Such training can be conducted either with the C3 system *off-line*, hence solely showing exercise information, or *on-line* with exercise information being superimposed on a live operational situation. When on-line systems are used, the exercise controller must be given the ability to switch instantly between the real world and artificial world should the need arise. Designing systems that can switch between the exercise and real world is a complex technical undertaking. All supporting databases must be duplicated to avoid the possibility that real world information in the database could be corrupted by an exercise eg. exercise munition expenditure reducing the real world holdings of the munition.

Senior military commanders and their principal staff spend considerable resources ensuring subordinates are properly trained and exercised. However, as a general rule, very little time is available to develop their own fighting command and control skills.

5.1.1.4 Simulation

Simulation at a tactical level is a relatively simple challenge. Such models incorporate weapon performance, have strong spatially-dependent characteristics and have structures based on the passage of time. The concepts of these models are straightforward and virtually universally agreed. However, at the operational and strategic levels there is no agreed framework, paradigm or model for C3 systems. In an attempt to develop a high-level model, as a starting point DSTO is considering many of the proposals of the Command and Control Reference Model (C2RM) developed by the US Army CECOM. It describes a generic framework for an object-oriented, open system architecture of resources networked and integrated to comprise a C3 system compatible with the International Standards Organisation (ISO) Open Standards Interconnection (OSI) reference model for Communications.

Simulation of higher level C3 systems cannot incorporate the details of every individual man, weapon or piece of equipment. Therefore simplifying assumptions need to be made in considering groups of entities (men, machines, weapons) instead of each individual. Attempts to summarise and simplify parameters and event descriptions, while keeping the implementation to tractable levels have, in the past, often included the imposition of smoothness and other constraints on the relationships between the parameters. Modern analysis techniques attempt to address these limitations.

The ultimate aim is to develop a C3 simulation which will provide a capability to conduct thorough examinations of C3-related procedures and technologies. It would enable the effects of proposed C3 systems to be examined within the framework of simulated military missions. Following the analysis of system performance characteristics, the next logical and necessary step is the determination of how such systems influence overall mission effectiveness. Such research will help in the determination of ADF user requirements and in the assessment of purchase and developmental options. It will provide the means by which the ADF can improve its ability to exercise high-level command centres taking account of operational and tactical level considerations. In addition it will provide the means for ascertaining the influence of current and proposed C3 systems on a wide range of military missions covering strategic, operational and tactical conflict levels and involving all three Services.

DSTO is building a Distributed Interactive C2 Effectiveness (DICE) simulation model. The following components of DICE are being developed:

- An interactive, object-oriented scenario generator. This will enable the conversion of specified military scenarios into the form required by the model, using user-friendly screen-oriented procedures and limited data entry;

- Techniques for interfacing, either on-line or off-line, with tactical battlefield simulations and war games;

- A multi-mode, variable time simulation controller. Simulations involving both wholly synthetic and combined real and synthetic decision-makers will be required. The controller in catering for these options will need to be able to adjust the rate of passage of time to suit constraints on decision-making and total simulation time;

- Synthetic decision-makers capable of correctly selecting from a finite range of options, given formalised input data. Techniques for incorporating artificial intelligence are to be pursued actively, and developments in this area monitored to ensure state-of-the-art decision-makers are used in the model;

- A highly cross-referenced database for interrogation, analysis and statistical summary. This will enable analysts and end-users to select a specific event, either during or after the simulation, and establish the conditions and reasoning leading to its occurrence. As a consequence, specific, possibly critical path, strings of events may be followed during post-simulation analysis; and

- A limited capability for distributed integrated simulation enables participants in a simulation to operate from convenient locations. Here regard will be taken of international protocols to ensure developments made outside the country can be readily incorporated when appropriate.

The system is currently being developed on SUN SPARC 10 workstations using UNIX and utilising a Silicon Graphics INDIGO ELAN for graphical displays. Commercial-Off-the-Shelf (COTS) software is used whenever practicable.

The DICE decision philosophy calls for a small number of miliary decision-makers, possibly situated at different geographical locations. To enable a realistic simulation of a military mission, numerous other decision-makers will be simulated. Considerable DSTO effort is being directed towards the development of realistic synthetic decision-makers. It is expected that AI research will produce improvements in this area cognisant of available data, protocols and constraints. A variety of decision-makers types are needed for any simulation, each able to carry out its allocated role with a high degree of realism.

5.1.1.5 Measures of Performance

The C3 process consists of people, organisations and procedures as well as the technology. The technology can be treated separately and can be evaluated using Measures of Performance (MOP). Elements of the communications system required to carry out our mission can also be evaluated using MOP. MOP enable parts of a C3 system to be evaluated in isolation. However, it must be recognised that optimising sub-systems does not necessarily produce the optimum overall system.

5.1.1.6 Measures of Effectiveness

An attempt has to be made to determine whether the system as a whole is effective and how sensitive it is to variation of the characteristics of the components. Given a Measure of Effectiveness (MOE) of the overall mission, the system should be able to conduct a series of simulations to determine how the C3 system affects the mission. Choosing an MOE that allows C3 system variants to be tried while not perturbing the rest of the system unduly, and thereby rendering conclusions about the effectiveness of the C3 system invalid, is a matter for careful deliberation.

5.1.1.7 Security

In the early 1970s the US realised the vulnerability of their C3 systems which held Top Secret information. In response, the National Computer Security Centre (NCSC) produced a revised security policy promulgated in the *Rainbow* series of documents – the most commonly used in this series being the Yellow Book for risk assessment and the Orange Book which classifies a system's security rating against specific criteria. These ratings range from *D* for minimal security, to *A1* for a fully-trusted secure system. At the time of conception, industry was expected to make available a whole range of products spanning the spectrum of security ratings. A fundamental tenet of these revised policies was that security has to be built in to a software product during development and can not be retro-fitted.

With hindsight it is becoming apparent that the NCSC philosophy underestimated several problems: first, the time required to validate software to a security rating above *B1* can be in excess of three years. It is common commercial practice that new versions of software are issued every 12 months with nearer six months being common in office automation. Hence by the time software is validated it is likely to be obsolete. This is a compounding problem in that if users attempt to keep up with new revisions, they will fall further and further behind. Second, as the user's security rating increases, the level of functionality decreases. While this may be frustrating for a user, it poses extreme problems in system administration. Finally, there is only a small list of products evaluated at the B1-level and above, including security guards and filters, Compartmented Mode Workstations (CMW), Secure Operating Systems, and Secure Database Management Systems. Very few products on the market have been evaluated above the B1-level, the only ones being very special-purpose applications. Their unique qualities make them costly to purchase and maintain, and their performance tends to lag behind the state-of-the-art.

In the late 1980s there was an overwhelming military requirement for trusted computing systems and the DSTO commenced development of *add on* security devices which could offer selected security functions. This research ran contrary to academic guidance that security could not be retro-fitted. The prime objective was to develop devices which could tightly control the flow of information and could be accredited a satisfactory level of trust. Such devices could either control the flow of information to and from an individual machine or more importantly allow interconnection of LANs. In the military environment there is a pressing requirement to be able to share information across LANs which may be operating at a different system security rating. For an ADF example, the currently planned LHQ is being designed to operate three LANs each physically separate and running at a different system security rating.

In order to assess the current trends in security as they pertain to the evolution of C3 systems, the four principal components of the security engineering process must be considered:

- Security Policy – the rules defining security;
- Security Mechanisms – the hardware and software components that implement the policy;
- Verification – Methods and Tools used to ensure the mechanism implements the policy in a correct and trustworthy manner; and
- Certification – the process of issuing a *seal of approval* for providing specific levels of trust.

The state-of-the-art with regard to security policy provides us with the principal ability to state the confidentiality of specific pieces of information. Research will continue through the next decade in a number of policy areas:

- Integrity – developing the ability to specify accurately the data integrity requirements of our automated systems;
- Assured Service – developing specification practices/standards to define the level of service assurance that is required from an automated information management system; and
- Federated Policy – developing methods to define the security policy for integrating (or connecting together) C3 systems that have been developed independently.

5.1.2 Information/Knowledge Engineering

There is a tendency to view an information system in terms of computers, communications and software applications, whereas in reality an information system is first and foremost the knowledge it encapsulates. Recognition of the centrality of information will see computer science move towards knowledge science rather than hardware and software which have been the traditional focus to date. Similarly information engineering, the application of principles to solve information-related problems will rise to prominence in the coming decade just as software engineering grew in the 1970s out of recognition of a crisis in software development.

5.1.2.1 Information Engineering

Information management has progressed from flat file systems, to relational databases, to integrating homogenous databases and, currently, to integrating heterogenous databases. The challenge of the 1990s is not integration but interoperation. It is now recognised that integrating all the databases in the world is not possible, and that what is required is a paradigm which will permit interoperation. Further this paradigm must also cover information that is not stored in databases. After all, only 5% of the world's electronically sourced information is from a database management system.

The paradigm of the 1970s and 1980s was data. This is being replaced in the 1990s by the paradigm of the object. The main issue for information management in the 1990s is distributed object management. Objects must be managed by the computer system to support the business processes of the enterprise. There is a clear merging between an enterprise's business processes and the information technology processes which support them.

Distributed object management relies heavily upon the need for information systems to co-operate in order to deliver the information required by an application. Co-operation requires that knowledge of a system and its relationship to other systems is embedded in the information system. The proposed paradigm for this is the agent although the implementation details for agents are still an area of active research.

The main stumbling block for future information engineering is associating semantics with the data or objects stored. Currently computer systems simply process data without having any understanding of the meaning of the information. Having an understanding of the information in a domain requires the representation of knowledge.

5.1.2.2 Knowledge Engineering

Knowledge engineering addresses how knowledge should be represented in a computer and how knowledge can be acquired. Our current ability to represent knowledge exists at the data and information level. In order to represent knowledge more fully, relationships have to be drawn between information which is appropriate to the problem at hand.

Representation techniques in the 1980s concentrated on the detailed knowledge of narrow domains. In the 1990s greater emphasis is being placed on representing common sense. This initiative attempts to overcome the fragile nature of systems which capture only very deep knowledge.

Several knowledge representations have been developed and there are now thousands of knowledge bases in the world. A key area for knowledge representation in the 1990s is how these diverse knowledge bases can be shared. Mechanisms for translating from one knowledge format to another are also being developed.

Knowledge acquisition has historically been a time-consuming and unrewarding task due to poor mappings between the expert's intuition process and the knowledge representations used by computers. Software packages to assist the knowledge acquisition process have been developed, but most simply store and track knowledge acquired from long and detailed interviews. Future systems for knowledge acquisition are addressing how knowledge may be acquired in the day-to-day operation of computer systems.

5.1.2.3 Informal Information Flows

Informal information flows play a significant role in the effective operation of higher level C3 systems. While it is a matter of intellectual conjecture exactly what constitutes informal information and where the boundary lies between informal and formal communications, the traits of informal communications are such that they cannot be predicted, usually they have no recognised procedure associated with the information and normally they are interactive peer-to-peer communications. As well, normally informal information flows have no audit trail.

The scientific community has been slow to offer support to informal information flows, although recent command analysis exercises have addressed this issue. IT support for informal communications flows have similarly been slow though arguably the telephone, fax and e-mail are useful tools. Video conferencing, video telephone and groupware products are future developments which will continue the trend of support to informal information flows. Until informal information flows are supported fully, a distributed C3 system will have an obvious deficiency.

5.1.3 Human Engineering

Human engineering can be considered as the comprehensive integration of human characteristics into system definition, design, development and evaluation. The aim is to focus on optimising the performance of human-machine combinations. With recognition that human users are an integral part of a C3 system and the increasing amounts of information which IT can make available to users, the human machine interface is increasingly likely to be a system performance limiter in future systems.

5.1.3.1 MANPRINT

MANpower and PeRsonnel INTegration (MANPRINT) is a methodology which attempts to integrate human factors into the total engineering and acquisition process. MANPRINT defines not only activities and deliverables, but also the composition and reporting structures of senior project management committees and steering groups. It addresses 6 domains:

- Manpower – staff required to operate, manage and maintain a system;
- Personnel – the skill level required by these staff;
- Training – the amount, cost and time required;
- Human Engineering – optimising human machine interaction;
- System safety – equipment safety; and
- Health hazards – environmental factors which may reduce human performance.

Traditionally these specialisations have worked independently on projects. MANPRINT, however, brings them together under one umbrella and more importantly tries to identiiy real cost and cost-savings that can be achieved in these domains.

MANPRINT has been used extensively by the US and UK military particularly on hardware-oriented systems. Despite its obvious overhead on development cost, it has been demonstrated to achieve significant cost savings overall (Reference 9 Booher 1990). Its potential weakness is that it is a large program and requires tailoring to individual projects. DSTO has conducted preliminary investigations and considers the methodology holds its greatest potential for future ADF systems in addressing Human Engineering issues within the Human Computer Interface.

5.1.3.2 HCI

Human-Computer Interaction (HCI) is a sub-discipline within the general field of Human Factors. It is concerned specifically with the human factors of the use of computers and includes both cognitive and physical aspects of such usage. HCI in C3 systems aims to harness and expand human productivity and creativity in C3 by matching the demands of products, systems and tasks to the physical and mental characteristics of those people who use them.

All new developments need to take advantage of the wide range of human sensory and motor capabilities in order to make interaction with computers more natural and efficient. Many HCI issues are related to these new developments which will require more research activities in the future. Specific areas that are being addressed at the moment include HCI using:

- Virtual reality;
- Natural Language processing;
- Hypermedia;
- Visualisation; and
- Groupware.

With growing technical complexity, there is growing awareness that the physical and mental capabilities of the user are going to be a limiting factors of system performance. As well, no matter how brilliant the technical concept and execution of a product or system, it is doomed to fail if the users for whom it is intended cannot or will not use it. HCI, therefore, is closely associated with a user-centred approach to system design and must be a consideration in future C3 system design.

5.1.4 Software Engineering

5.1.4.1 General Trends

The software engineering fraternity is overwhelmed by tools and methodologies. There is a growing awareness that simply creating new technologies is not going to address key problems and difficulties. Therefore, there is less emphasis on creating general analysis, design methods, and new languages, and more effort being directed towards:

- Experimentation and Measurement

  Each new technology is presented as a *silver bullet* but without hard evidence of the benefits claimed. Hence there is a major focus on experimentation and measurement to try to quantify the productivity and maintainability benefits of individual methodologies.

- Process and Product Improvement

  The intention of Process and Product Improvement is to generate a better understanding of measuring and improving the process and products of software engineering. An example is the Capability Maturity Model.

- Standardisation

  There has been a flurry of standards activity to help support the application of software engineering practices and principles. Most previous standards have focused on product aspects, e.g. the contents of software design documentation. The current trend is towards supporting the process.

- Professionalism

The distinction between computer science and software engineering is becoming more apparent. The trend is towards establishing software engineering as a legitimate profession in its own right.

- Visual programming

  The current trend is less emphasis on the language and more focus on the development environment and infrastructure. Integrated tools, data interchange and object-linking and reusable components such as supported by Visual C++ and Visual Basic are examples of this approach.

5.1.4.2 Middleware

The thrust in information systems implementation is to standardise those aspects which are common across applications, in a vendor-independent way. The term *Middleware* has been given to these services that sit between the operating system and the application. Although of recent origin, the term is in danger of becoming overloaded. Middleware services include the following:

- Presentation Management: forms managers, graphics managers, hypermedia linkers and tools, printing services manager;
- Computation: sorting, math services, internationalisation services, data format conversion services, time services, security facilities;
- Information Management: directory services, file and record managers, database management systems (relational and object oriented), repository services;
- Communications: Remote Procedure Calls (RPC), peer-to-peer messaging, queued message services, electronic mail, electronic data interchange;
- Control: thread manager, transaction manager, resource broker, fine and coarse grained scheduling;
- Distributed Computing/Interoperability services; and
- System Management: accounting, fault detection.

Distributed Computing Environment (DCE) is a set of middleware tools that provide many of the building blocks needed in building heterogenous, autonomous, distributed, (HAD) systems. DCE has been endorsed by all the major Open System vendors. The components of DCE are:

- Distributed File service, allowing processes to access remote files, transparently;
- Remote Procedure Call service, allowing processes to call procedures set up in other, remotely running, processes. This service underlies many others;

- PC Integration service, allowing processes to access PC-based files and printer resources;
- Time Service, providing system-wide time synchronisation for those applications that require it, even though local, unsynchronised clocks may be running in each system component;
- Security Service, allowing clients to access services and for proper authentication to occur. The server must know that the client is authorised to access the service, and the client must know that the service is and does what it represents itself to be and do;
- Distributed directory service, which provides an index of network resources. This integrates the X.500 global naming system with a fast replicated local naming system;
- Threads service, allowing large increases in the number of simultaneous clients for any service; and
- Network Management.

5.1.4.3 Distributed Databases

Distributed Database technology is concerned with making a number of distinct database systems appear like a single database system to a user. The need for this technology arises frequently, as a consequence of the need to distribute data geographically, or as a result of the need to integrate different software development efforts.

The term is often restricted to multiple databases having identical structures where the same database software system (DBMS) manages each database. The term Federated Database is often used where databases have different structures and contain different types of data. For example traditional relational database systems contain formatted data where entities and their attributes are represented by records having predefined fields; geographic database systems represent the geometric and topological properties of geographic objects; text database systems represent structured or unstructured text data, etc. Object databases subsume all of the above.

There are two major classes of problem that have to be solved in deploying distributed database technology successfully. These are distributed query processing, and distributed update.

In distributed query processing, the user should not have to know the physical location of the data being retrieved. In addition, retrieval requests involving relationships which cross actual database boundaries should be handled automatically.

An update may involve changes to a number of different constituent databases, and all of these must occur to leave the database in a consistent state. Informally, retrieval requests following the update must see the whole update. Technologies to handle this are provided by Distributed Transaction Managers (DTMs) and constituent databases which adhere to recognised standards.

5.1.4.4 Integrated Programming and Software Environments (IPSEs)

It is increasingly recognised that a system's life cycle must be considered as a whole, rather than being divided into independent stages. This division has arisen previously for a number of reasons, including procurement practices and the inherent differences between, say requirements-definition and coding. Nevertheless, as procurement cycles are shortened, particularly with Evolutionary Acquisition, the integration of different life cycle phases becomes more important. Integration may also become easier with system development paradigms such as Object Orientation. Some specific issues being addressed include:

- Use of Object Orientation to provide vehicle for more seamless integration between life cycle phases.
- Tools to provide more flexible updating of requirement, design and coding specifications, so the influence of one phase can be assimilated in another.
- Provision of Life Cycle Support facilities, specifically targeted at providing whole life support to C3 systems.
- Cross-compatibility between representations and methods to ease re-engineering tasks if multiple methods have been used.

5.1.5 Hardware Engineering

5.1.5.1 Processors

The salient characteristics of the 21st Century battlefield are high-mobility, rapid decision-making, an integrated picture of the battlefield that is common throughout the area of operations and dispersion of C3 assets. All these features are demanding improvements in computer processing power. Every part of a C3 system, from user-interface to frequency synthesis, and from coding algorithms to signal-processing, depends on processors. The need to package more capability (pattern recognition, artificial intelligence, information/data filtering and correlation, etc.) into a piece of C3 equipment greatly increases the processing work-load. Processors must therefore become smaller, faster, able to load share through parallel operation and, because they will be appearing on the battlefield in ever-increasing quantities, less expensive.

Commercial production of processors can be categorised in one of three architectures:

CISC

Complex Instruction Set Computer (CISC) is a mature architecture for processors. Its fundamentals are a complex and powerful instruction set. However, to achieve greater performance, this architecture is tending towards greater complexity. An example of CISC architecture is the Intel 80X86 series used in personal computers.

RISC

Originally an IBM development, Reduced Instruction Set Computer (RISC) aimed for a simpler architecture, fully scalable, with fewer instructions and more uniformity. RISC architecture is characterised by one instruction per clock cycle, fixed format instructions but with the penalty of increased compile time effort. Due to the relative simplicity of RISC hardware, it is significantly cheaper to produce but invariably is priced in the market comparable to CISC processors of simpler power. An example of a modern RISC chip is the 64 bit DEC Alpha which can achieve 300 million instructions per second.

Multi-processor

The performance of single chip processors is primarily limited by the chip construction process. Since better performance generally translates into greater circuit complexity, high-performance processors usually require more transistors per chip than less capable processors. Because the size of etching beams is approaching the size of chip features, current X-ray lithographic techniques will not support major increases in complexity. Further improvement will have to come from migration to higher-frequency etching beams. Electron beam lithography is now being considered. Even if electron beams prove to be successful for mass chip production, increased stray capacitance due to the closer proximity of chip features may limit the operational frequency. Successful research in feature geography, together with new semi-conductor materials such as Gallium Arsenide, will be needed to overcome these problems.

To overcome these inherent limitations, it is possible to implement multiple-processors on multiple pieces of silicon. The main limitation of multi-chip processors is the relatively large distance separating individual components. This separation introduces propagation delays and stray capacitances, both of which limit the operational frequency. These variables can be minimised, but not eliminated, by optimising the topology of processor circuit cards. The increased number of solder connections also presents a reliability problem, especially in harsh environments. Given the greater number of ways to increase performance, the reduced space requirements, and the fewer solder connections, single chip processors appear to be preferable for future tactical systems and hence warrant a concentrated R&D effort to overcome chip construction obstacles.

The multi-processor architecture is usually RISC-based technology with processors arranged in a matrix architecture to allow parallel processing. The transputer is an example of a processor intended to be used in this role. Such architectures have very high processing power potential but require complex compilers to harness this potential. The compilers must be able to isolate task entities, to sub-divide tasks and to co-ordinate execution of tasks. Consequently, the performance of this type of architecture is very task-specific. Examples of tasks to which this type of processing is suited would be classifying raw sonar data, high-speed signal-processing, deciphering coded messages and virtual reality.

An example of a parallel processor is the Scalable Array Processor (SCAP) recently developed by DSTO. The SCAP is essentially a matrix engine in which calculations are performed in parallel rather than sequentially. The processor has been demonstrated and currently faces the hurdle of moving into full production. The basis of the SCAP chip is VLSI technology: 20 processors are tiled across the chip surface and then 20 SCAP chips tiled on a circuit board, giving a total of 400 processors. The intention is to build the SCAP processor into a desk-top machine to give super computer performance at a total cost of less than $100k.

The trend in processors will be directed in the commercial market place. The power/cost performance ratio is in favour of RISC computing and hence it will likely win. However, there will be enduring specialist niches for the more expensive multi-processors solutions and even custom-designed Application-Specific Integrated Circuits (ASICs).

5.1.5.2 Mass Storage Technologies

Due to its low cost, traditional magnetic storage will have an enduring role where access speed and ruggedness is not critical. At the tactical-level, highly-mobile C3 systems will involve the storage, retrieval, and modification of large quantities of data at battalion level and below. This means the devices that store data must have read/write capabilities and be rugged enough to be dropped and submersed, yet small enough to fit in a soldier's shirt pocket. Events at the tactical level can physically disturb the disk drive during critical activities like movement of the read/write heads. Small, static mass storage devices will be essential to the 21st Century C3 systems. Although there are a number of promising static mass-storage technologies, each has one or two obstacles, some significant, some not.

Mass storage technologies can be sub-divided into three areas, being;

- Magnetic;
- Optical; and
- Semi-conductor.

Magnetic

Magnetic storage devices offer a complete range of capabilities but broadly performance is directly proportional to cost. At the bottom of the range is reel-to-reel tape which is very cheap but due to its serial nature is very slow. The floppy disk is a universal medium with 1.44MB devices being the current norm. In the near future 20MB floppies are expected to be available. The floppy optical is a subtle development of the standard floppy, in that an optical-based head positioning system is used permitting much greater magnetic packing densities. A typical 3.5" floppy optical disk can currently store 20 MB of information and devices up to 650 MB are expected in the near future. Hard disk drives offer several Giga Byte storage with access times of a few milli-seconds. However, the main trend in the commercial sector is miniaturisation of hard disk drives that consume less power and have greater ruggedness. Such devices are required in hand-held consumer IT devices. Magnetic Bubble memory was commercially developed in the 1980s but due to its high cost is used only for specialist applications. It is inherently robust, non-volatile and has a capacity in the 100s of Kilobyte region. However, it has the drawback that temperature extremes can cause loss of data.

Optical

Optical devices permit about 1000 times the data density of floppy disks. The most widely currently used device is the CDROM. This 5 1/4" disk can store in excess of 500 MB of data and is inherently rugged. Re-writible CDROMs are just beginning to appear in the commercial sector. A cheap alternative is the WORM – (Write Once Read Many). This is similar technology to the CDROM and is ideally suited to archiving stable permanent data.

Present optical memory devices store one-dimensional information in a two-dimensional space. Using a two-photon, three-dimensional approach, photochromic materials are being developed by US researchers that offer more than 18,500 times the storage capacity of conventional approaches. Small enough to be incorporated onto standard computer boards, these optical computer memory systems will be interfaced to advanced computer architectures for high-speed numeric and symbolic processing in military applications. The technology shows the potential of storing one terabit of information (1,000,000,000,000 – bits) in a form the size of a sugar cube with no moving parts. In essence, this informational sugar cube could potentially store the equivalent of 2.4 million floppy disks – with all information retrievable at the speed of light.

Semi-conductor

Semi-conductor storage is unlikely to ever be as cost-effective as alternative magnetic and optical storage devices. However, it is extremely robust and is therefore favoured for some military applications.

There are two varieties of Random Access Memory (RAM) – static RAM (SRAM) and Dynamic RAM (DRAM). Both types are inherently volatile, that is, they require continuous power to retain data. Additionally, data stored in DRAM must frequently be refreshed, since it is actually stored in minute capacitors that lose charge with time. SRAMs are very fast, with read/write times in the tens of nanoseconds (ns) or less. DRAMs are not as fast, exhibiting typical memory-access times in excess of 50 ns. Battery-backed SRAM cards were the first static memory cards to be used for mass data-storage, but are relatively expensive on a cost-per-byte basis. The reason is that SRAM data-storage cells are large, production yields are low, and SRAMs have not been produced in large quantities. Cost-effective manufacturing technology is a challenge for

SRAM mass storage devices, one that may never be cleared because more promising technologies are on the horizon.

Current semi-conductor memory can give 4 MB of DRAM (Dynamic Random Access Memory) in a volume of 4 cubic centimetres. Credit card sized memory cards with 20 MB of storage and battery back up are now available commercially.

Electrically Erasable Programmable Read Only Memory (EEPROM) is a non-volatile memory technology with extremely fast access speeds. However, EEPROMs have limitations. First, they require an extra power source for erasure; some chips use an on-chip charge pump to produce the necessary erase voltage, but this adds greatly to the price of the chip. Second, the reliability of an EEPROM chip drops drastically after 10,000 read/write cycles. Finally EEPROMs are slow (80 ns) and expensive (about 8 to 12 times more expensive than DRAMs). Flash-memory is a variant of the EEPROM and is a non-volatile memory technology that hol [illegible] for the 21st Century systems. Flash-read access times are on a par with DRAM read access times, and represent a 100-fold improvement over magnetic media. Although present flash-memory costs three times as much as volatile memory, in theory, it can achieve the same density as DRAM at comparable cost, once mass production begins. In addition to overcoming the cost problem, design engineers must find ways in the years ahead to speed up flash-memory write-times (currently about equivalent to that of conventional magnetic disks) and to allow flash-memory Integrated Circuits (ICs) to be programmed bit-by-bit, rather than sector-by-sector. It is expected that flash-memory at a cost of $100 per MB will be available soon. Again these devices will be credit-card-sized.

It is expected all these memory technologies will develop in parallel with no outright winner as such. As a general rule magnetic technologies will always be vulnerable to temperature extremes and precision drive mechanism will be susceptible to mechanical shocks and vibrations. Optical technologies are more robust than magnetic devices as they have some immunity to head crash. However, the small, light-weight, high-density solid-state devices are likely to remain comparatively expensive and therefore are used only in specialist applications.

5.1.5.3 Display Devices

One of the great hurdles to be overcome by future C3 systems is producing display technologies that can equal the resolution of a photograph or printed map. Most screen technologies can support only approximately 300 Dots Per Inch (DPI). The latest laser printers can mange 1200 DPI. While unquestionably screen and laser printer technology will improve it is unlikely in the near term they will equal 2000 DPI, the resolution of a good quality map.

The conventional Cathode Ray Tube (CRT) remains the dominant display since the invention of television over 40 years ago. No other medium offers the speed, versatility and interactivity necessary for the display of text, graphic imagery or video. Many attempts have been made to squash the CRT, to improve its resolution and to decrease its power consumption but in general these attempts have either reduced the quality of the image or lead to excessive manufacturing costs.

Plasma displays

Plasma displays consist of a matrix style array of miniature neon lamps that are discharged by a combination of row and column voltages. A refinement is the alternating current plasma display which uses insulated electrodes which retain the triggering charge and hence have a memory-like effect. A similar technology is the thin film electroluminescence display which replaces the gas of a plasma display with a phosphor film.

Plasma displays can be fashioned into flat screened panels up to 1.5 meters long which will support a visual resolution suitable for high definition television. Although these displays are inherently durable they consume too much power for portable applications and generally cannot provide full colour response.

Liquid crystal displays

These displays make use of organic molecules known as liquid crystals. The basis of operation is to sandwich the liquid crystal between glass sheets having different polarisations. In an unenergised state, light travelling through the polarising glass is twisted as it transits through the liquid crystals and exits the sandwich, i.e. the *on* state. If an electric field is applied through transparent electrodes on the liquid crystal, its molecular structure aligns and no twisting of the incoming light occurs and hence no light is emitted – the *off* state. A matrix of these cells forms an array of tiny electronically controlled shutters. Colour is achieved by grouping one cell dyed with each of the primary colours into triads. Addressing each cell can be done passively, that is, column and row voltages are arranged to trigger individual cells. However, passive triggering has an inherent problem that resolution can be improved only by sacrificing contrast. To overcome this limitation, one modern variant is the active matrix where each liquid crystal is switched by a thin film transistor.

Active matrix liquid crystal display can now rival the CRT for small-to-medium sized desk-top machines for image quality. Many users prefer the jitter-free crystal displays. Liquid crystal displays are ideal for miniaturised, robust displays.

Flat panel liquid crystal display will continue to evolve towards higher resolution, reduced power requirements and less weight. Such flat panels will likely become the norm for desk-top machines before the end of the decade.

Large screen displays

The most promising avenue for large screen displays probably lies with building matrices of conventional displays. Depending on the number of displays used, the amount of video memory and processing power needed can be enormous but is made a viable option by the decreasing cost of these technologies.

5.1.5.4 Fault Tolerant Hardware

The pace of battle in the 21st Century will not allow much time to correct errors introduced by information transport and management systems. Consequently, these systems must be fault-tolerant. To the extent possible, they must prevent faults from occurring. This means building redundancy into the systems. In those instances when faults cannot be prevented, the systems must manage the faults by detecting and correcting them or, if correction isn't feasible, providing alternative service.

Fault management is composed of four sub-functions:

- Fault detection;
- Fault diagnosis;
- Fault correction; and
- Fault administration.

Fault detection includes the scanning of incoming status information to detect failures, the generation of alarm displays, and the filtering out of any duplicate fault reports. Fault diagnosis attempts to identify the extent of service impairment, to determine the cause, and, when necessary, to initiate any available alternative service. Fault correction uses predefined steps to attempt to restore the failed item to service. (These steps could range from shutting down an over-heating component, automatic replacement of the failed items, generating new code that will resolve software bugs, through to summoning maintenance personnel to the failure location). The fault administration sub-function logs faults for historical purposes and predicting trends that will be used to update fault diagnosis and correction rules.

Because of the harsh battlefield environments, fully automated fault management for military systems may not be possible by the 21st Century. This is true for two main reasons. First, tactical network topologies tend to have a number of dead-end tentacles that preclude initiation of alternative services and limit fault diagnoses. Single-threaded communications links have no alternative-routing capability and failure of such links will cut off all automated status information from equipment beyond them. Second, the possibility of catastrophic destruction due to hostile action greatly impacts the extent to which fault management can be implemented. For example, if a computer goes down because the enemy destroyed a generator, there can be no automated fault correction or reporting, unless the system has an alternative power source that survives the enemy action.

Careful study of fault management for military information management systems is necessary before extensive automation can be implemented. The study must ensure that 21st Century fault management concepts are suitable and cost-effective for a battlefield environment. It must weigh the criticality and time-sensitivity of each information management system against the expense and anticipated capabilities of new fault management technologies (such as AI). It must consider the fact that military systems will still be operator-attended and therefore can be quickly and easily maintained on a manual basis, provided the operators are maintenance-trained. Through study and review of factors such as these, the major obstacles to automated fault management will be overcome.

Redundant Array of Inexpensive Hard Disk Drives

The aim of Redundant Array of Inexpensive hard disk Drives (RAID) is to avoid the failure of one hard drive causing system shutdown or loss of data. In the event of a single disk failure, data on the defective drive is automatically regenerated from the remaining drives and the user can continue to use the system. Such systems normally consist of 3 to 5 disk drives and can operate with minimal impact on system performance.

Redundant Chip Technology

Fault tolerance is already manufactured on some chips in that redundant circuitry is fabricated on the silicon waver and after testing links are cut or fused to configure a chip to use only error-free parts. This is clearly not a very sophisticated process since it can be performed only at the time of manufacture. Future chips may be reconfigured while in operation.

Most RAM systems now use Error Correcting Codes (ECC) to self-test their status. If faulty memory areas are found, they are by-passed automatically.

System Duplication

Systems have been available for a number of years with full circuitry redundancy and fully duplicated processing – Tandem and Stratus perhaps being the most well known. These systems are difficult to design to ensure that there is no single point of failure or catastrophic failure mode. As well they tend to be very expensive and tend to lag behind latest developments in processors. Due to their expense, they are probably suitable only for safety critical systems (aircraft, ship navigation) or in high value switching nodes.

An alternative approach is to use clustering technology which can allow load-sharing among processors and ensures that if one fails the load is picked up by the other processors. The whole operation is controlled by software which normally forms an extension to the operating system. For military C3 systems, it is questionable whether it is wise to rely on even fully fault tolerant systems if all the hardware is in the same building or even on the same site. With high bandwidth networking, clustering can be employed across geographically dispersed sites.

5.1.5.5 Photonics

Photonics is the use of light, or neutral photons, to replace or work with electricity, or charged electrons, for processing, storing or transmitting information. Streams of photons can pass near or even through each other without encountering or creating interference. This property means cleaner transmissions that are free from any form of crosstalk. Photonic devices have the potential to be faster, carry and store more information and are less susceptible to noise or electromagnetic interference than electronic devices. Hence, from a military standpoint, this technology has the potential to significantly improve the performance in many areas of future C3 systems.

The worldwide consensus among scientists is that photonics may lead to a technological revolution in the 21st century just as electronics revolutionised the 20th century. In the US, electronics is a $200 billion-a-year industry and growing about 10 percent annually. In comparison, photonics is a $10 billion-a-year industry growing at a rate of about 50 percent annually. Predictions indicate the growth rate of the electronics industry will decline, while the growth rate of the photonics industry will remain at about 50 percent annually for the near future.

Photonics can be addressed under four main application areas:

- Telecommunications;
- Optical Storage and Display;
- Sensors; and
- Information Processing

Telecommunications
Fibre optics is firmly established for long-distance communications by virtue of its large information capacity, distance between repeaters, and freedom from electrical interference. Advances that are likely in the near term include improved optical switching components and optical amplifiers.

Optical Storage and Display
Optical storage media offer very high density storage. Optical memory can store data in three dimensions. In a three-dimensional or holographic memory, information is partitioned in binary planes that are stacked in the third dimension. One memory operation is performed on the entire plane of bits, thus achieving a tremendous memory bandwidth increase over conventional two-dimensional bit-oriented memories. By storing information in volume media, optical three-dimensional memory can achieve very high density in a very small space and allow very high access times. In addition, no moving parts are involved making such memory robust from a military perspective.

Photonic displays are those addressed by light beams, as when a laser writes on a liquid crystal cell. Such displays have specialised uses but are not likely to displace existing electronic display technologies in the foreseeable future.

Optical Sensors
Photonic sensors include fibre-optic sensors and Focal Plane Arrays (FPAs). The former have been developed for sensing of temperature, pressure, displacement, magnetic fields, and other physical or chemical environmental parameters. They are accurate, can operate in harsh environments, and are compatible with optical telemetry. High-performance fibre-optic hydrophones, gyros, and magnetometers have been demonstrated for many military applications. FPAs using primarily charge coupled and charge injection device concepts have, in the last two decades, led to a revolution in data handling and processing of radiation-induced signals in the infrared and visible regions. Research is continuing into improved materials, interfaces, and fabrication yield.

Information Processing
Photonics offers the potential advantages, for both analog and digital applications, of almost limitless bandwidth. Today's typical computers move data down a bus 32 or 64 bits wide. With photonics, bus widths of 10,000 have been suggested. The present use of photonics in digital information processing is largely in the interconnections: computer to computer and computer to storage input/output device. These interconnection networks will become more critical as computer architectures migrate toward distributed multi processors. High-speed, high packaging density, and high reliability photonics compatible with the electronic integrated circuit technology used in computers has yet to be developed. Hybrid approaches to integration of the electronic logic and the photonic interconnects are promising for the near term. However, hybrid solutions still require processes that can covert electrons to photons and vice versa which is an intrinsically slow and difficult operation. Monolithic integration is the ultimate goal but is unlikely within next fifteen years.

There is much present interest in the question of all-photonic digital computation because of the fast response of optical devices, but this is still very much in the research stage. The University of Colorado recently demonstrated a prototype optical computer. It was able to multiply a 100 element vector by a 100 by 100 matrix in about 20 nanoseconds. However, by their judgement, the prototype is many years from the market place. More research is needed on materials with larger nonlinearities, on new algorithms, and on new architectures to match the special characteristics of optical logic elements.

5.2 Enabling Applications and Tools

5.2.1 Office Automation

Office Automation (OA) is rapidly improving in functionality driven by the enormous demand and hence potential profits in the commercial marketplace. Examples of these developments are word processing becoming indistinguishable from desk-top publishing, spreadsheets supplied with advanced simulation and analysis capabilities, business and presentation graphics tending towards CAD and other professional graphic designer capabilities, and database access, mail, fax interfaces over networks.

User interfaces are designed to be intuitive requiring minimal training of operators. However, training and support can be a challenge for advanced features of these packages. One of the problems is that an average user may in fact use only a small fraction of a program and hence there is a growing requirement to be able to tailor OA packages to optimise performance and efficiency.

Market leaders in OA package solutions are Microsoft Office, Lotus Smartsuite, and Aster*X. However, even these are all tending towards a common look and feel. Improvements expected in the near term improved filtering packages to allow export and import of data from other packages although Standard General Mark up Language (SGML) will assist with text-based document exchange. Other features that are expected to improve are common macro language across packages and development tools to exploit capabilities of packages. Portability of packages across a range of platforms is an area in which improvements are imminent. Future AO packages will probably be able to coexist with any mail transport layers including X.400-based systems.

Object-embedding technology (e.g. Microsoft OLE) has great promise but presents a number of administrative problems. Examples of embedded objects include maps, images, video and audio. Hot links (for example linking the results of spreadsheets) present security issues that will need to be addressed. Fault-finding particularly with objects distributed across a network will be difficult task as well.

A significant problem at the higher levels of C3 systems is organising briefings and meetings. A number of OA packages support networked electronic diary systems and if used widely by command centre personnel scheduling meetings would be easier and more effective. Electronic diaries are available with the required functionality but they are generally more difficult to use than their paper equivalents. However, future electronic diaries will be easier to use and hence will gain wider acceptance.

Modern OA packages normally have powerful macro languages attached. Hence OA packages have the potential to be used as the glue to integrate legacy *stovepipe* systems.

5.2.2 Groupware

The 1980s are said to have been characterised by *me*, while the 1990s are being characterised as *us*. This observation cn social matters is also reflected in the computer world, with a variety of COTS products available in the 1990s which provide group-working productivity tools rather than the individual productivity tools of the 1980s. Once individual staff within a Command Centre have reasonable productivity tools, the organisational effectiveness of the Command Centre as a whole is best enhanced by individuals working more effectively as a team. This *team* notion can then be expanded to include external groups within a multinational force. Some issues being addressed are:

- Enhancing responsiveness of groupware, so that project teams and ad hoc groups can be set up quickly and dynamically as the situation demands;
- Integration with individual productivity tools, so the groupware does not require a whole new set of facilities;
- Providing groupware products which can cross operating systems and communications boundaries, for international collaboration between different groups; and
- Expansion from current focus on relatively straightforward tasks (meetings, group authorship and so on) to include knowledge-base and information-base sharing.

5.2.3 Multi-Media

Multi-media techniques have the potential to revolutionise near future C3 systems. The multi-media approach is not only an issue of the user interface, but also an extension of a system's functionality. Multi-media can be defined as a system that merges the modalities of text, voice, still images, motion video and animation. Each multi-media system may not contain all these components, while others may contain them all as well as other features such as hand-written input and touch screens.

Multi-media systems enhance the way the people are able to communicate with each other and with their computers. This is because multi-media systems allow redundant coding (the same message on more than one channel, e.g. video and audio) which results in more effective presentation of the information for human processing.

The trend is that C3 systems will increasingly require the integration of many types of media in a coherent and intelligent way. A limiting factor will be provision of telecommunication infrastructure that will allow the high bandwidth that multi-media systems needs, for example, to support desk-top video conferencing. DSTO is addressing the following multi-media related research areas:

- A means of navigating the complex information via concept linking; and
- Human factors research in the design and usage of complex multi-media systems.

5.2.4 Hypertext

A hypertext document is one which supports the electronic linking of information/concepts within or between documents and thus allows users to read text on the basis of the links they have chosen. Links can be regarded as nodes in a web of information. These nodes can be created either on the basis of explicit and implicit links within the text. Hypertext is neither a mere electronic page turner nor is it a system which relies on text retrieval technology even though both of these facilities may be provided.

A hypertext system can also be regarded as an Human Computer Interface (HCI) to the information contained within a document or series of documents. Most instances of hypertext as an HCI conform to either the book or file card analogies, i.e. the behaviours of human users of these respective interfaces are consistent with the behaviours used to access information from books or file cards – activities with which the users of such systems are familiar. Note that the result of this is that the hypertext system is intrinsically easy to use requiring no usage of obscure Boolean operations (although Boolean search functionality is usually included in a hypertext system).

Important areas expected to improve in the near future are:

- The navigation problems of hypertext – *being lost in hyperspace*;
- A standardised text exchange format, e.g. SGML; and
- A language to describe the hyperlinking, e.g. HyTime.

In the next 15 years more complex hypertext areas expected to improve are:

- Automatic link creation; and
- The problems of maintenance of information and links in versioning.

5.2.5 GIS

A geographic information system (GIS) is an information system applied to geographical data. A GIS differs from other applications in that it has the ability to perform spatial reasoning. A GIS's information requirement can be divided into three broad areas:

- Terrain intelligence – natural features of the terrain;
- Environmental data – such as climate and weather; and
- Infrastructure information – man-made features.

Military systems are increasingly dependent on GIS services for their effectiveness, for example, navigation and guidance systems, surveillance systems, weapon-targeting, intelligence collection, and C3 situation awareness displays.

The fundamental problem to ali GISs is source data. Advances in remote sensing techniques are easing the problem. However, in an ideal world, data would be exported from data-gathering systems and imported into operational systems in a standard form. In reality this is rarely the case leading to the possibility of discrepancies in conversions. Hence there is a focus in DSTO on developing a data management strategy for the efficient and effective supply of digital geographic data for direct input into operational systems.

5.2.5.1 GIS Reference Systems

Prior to the ADF adopting the international standard of World Geodetic System 1984 (WGS84) which is based on satellite observations, the Australian National Spheroid (ANS) based on celestial observations was used. The two map systems currently in use by the ADF are:

- The Australian Map Grid (AMG) - based on AGD66 (Australian Grid Datum 1966 based on the ANS); and
- The Universal Transverse Mercator Grid - based on WGS84.

Provided users are aware of which standard they are using, electronic GISs can convert differently referenced single-point-data. However, the majority of GIS source data covering the ADMI was collated prior to 1984. The sheer bulk of this data makes it impracticable to convert all this legacy information to the WGS84 reference. The situation becomes more complex when the multiplicity of foreign geographic reference systems is considered. Hence within the time frame of this report, C3 systems will have to have the ability to work with multiple geographic references.

5.2.6 GPS

The Global Positioning System was conceived by the US armed services in 1973. The concept operates on a constellation of 21 satellites in high altitude orbits (20,000km) in six planes which give a GPS receiver, anywhere in the world, the ability to calculate its position in all weather conditions. The satellites transmit two signals: a C/A code intended for civilian applications offering positional accuracy to within 100 m, or an encrypted P code (known as Y code) intended for the military, offering 10m or better accuracy although both of these official figures are routinely bettered in practice.

GPS can also be deployed in a differential mode (DGPS), that is, a stationary GPS receiver is placed at a known location. This fixed station computes errors in the satellite signals and transmits corrections to a remote, possibly mobile, GPS receiver. By combining the GPS reading at the remote location and correction data from the fixed reference site, accuracies of 2m or better can be achieved using the C/A code.

Each satellite transmits a unique code allowing a receiver to track them independently. The GPS receiver measures the time of arrival of each signal and combining this with the known position of each satellite, it is able to calculate positional information, speed and exact time.

The military applications of GPS seem limited only by the imagination. Examples to date would be navigation, target acquisition, weapon guidance, artillery registration, sensor emplacement, annotation of photo reconnaissance and search and rescue.

With technological advances, the weight, size and cost of GPS receivers has reduced dramatically. Hand-held devices are now available to the general public for under $1,000. Improved signal processing techniques are also increasing the accuracy of the system. The trend will be to embedded GPS receivers in military systems of the future, for example mobile radios which can function as automatic position reporters, perhaps feeding information back to a C3 situation awareness display.

5.2.7 Retro-fittable Security Devices

An example of a retro-fittable security device is STUBS developed by DSTO and currently being commercialised by an Australian company. STUBS comprises two main functional components. First, the *Sealer* connects via a standard SCSI/RS 232 connection between a computer workstation and any communication link. The Sealer does not impinge on any existing infrastructure. Using a combination of smart card and PIN (Personal Identification Number) the Sealer permits selected operators with the required privileges to transfer information from a higher security workstation to a lower classified network. In doing so, it leaves a tamper-proof audit trail of the operators actions. The second component is a *Gateway*. The Gateway connects between networks and checks a tamper proof exit visa of information leaving a network and refuses to transfer information that has not originated from a STUBS terminal. The STUBS is designed to meet TCSEC A1 (ITSEC E6) level of assurance.

5.2.8 Cryptography

The traditional role of cryptography is to provide security to information as it travels over physically unprotected channels. Encrypted data offers a level of trust that the information has neither been eavesdropped or modified by unauthorised bodies. Encryption can be applied in many areas of modern technology such as protecting access to systems (e.g. by the use of unique digital signatures), protection of stored information and reduced probability of detection of communications (e.g. frequency hopping radio). The military has an enduring requirement for data and system protection and hence uses encryption widely. However, the current trend is for organisations such as banks, law enforcement agencies, commercial businesses and doctors to demand similar levels of protection for their data and systems. To meet the market need, the military has tested many cryptographic solutions which are readily available.

The types of systems into which cryptography is embedded are becoming increasingly complex. In the past, point-to-point leased lines have been the normal way of inter-connecting remote computers. The modern philosophy is to inter-connect computers using packet-switch technologies over public communications networks. In such complex networks there may be different levels of access depending on security classifications. These networks raise the problems of key management which are on a completely different scale from the traditional systems. Systems must now be designed with an electronic key distribution and multi-level security accesses while at the same time maintaining a unique encryption process where necessary between any two nodes on the network.

No practical cryptographic system can guarantee total security. However, an encryption algorithm can be made sufficiently complex that it would take an attacker an inordinate time to recover the raw information, given the attacker's resources. Computing power is becoming cheaper and more freely available, hence this alone requires more complex cryptography to ensure the same degree of protection. The variety of new data types (e.g. voice, fax, video, computer data and multiplexed signals) now being encrypted, and the speed at which the encryption must be done is another challenge for designers of cryptographic equipment The need for higher transmission speeds further compounds the requirement for greater complexity in the cryptographic algorithms.

As a result of many of the above points, cryptographic algorithms in the civil domain are now frequently being implemented in software. This raises new problems. One is the *trustedness* of these implementations, particularly in systems which must be secure. The heart of all complex cryptographic systems lies in mathematical operations on random numbers. Therefore there is the need for suitable cryptographic strength, as well as the traditional statistical randomness, to be incorporated into random number generation.

5.2.9 Voice-Input/Output

A natural language interface to C3 systems offers the advantages of a natural, hands-and-eyes-free interface which permits a faster alternative to the keyboard for information-exchange and instructions. Two technologies are required to support natural language interfaces, namely speech recognition and speech synthesis.

A typical speech recognition system has five basic building blocks. First, a Signal Processor drives a recognition sub-system which functions by searching a Speech and Language Model the output of which is fed into a Language Understanding Module responsible for controlling the final application. While there have been rapid advances in all these five areas in recent years the most complex and yet to be fully resolved is the Language Understanding module since the process of human language still contains many unknowns. Other difficult areas are the technologies to recognise phonemes and processes to eliminate speaker and environmental variabilities. It is an extremely complex task for a system to detect and reject transient noises and random conversations while recognising continuous speech. Systems which recognise single commands, such as hands-free dialling associated with mobile telephones are relatively easy to achieve and could be considered mature technology. However, systems which can recognise continuous speech are in their infancy primarily due to the difficulty of context-recognition within natural language.

Speech synthesis is at a more advanced stage. Many systems are available which use a dictionary-based vocabulary. Other systems derive acoustic realisation from phonetic base forms accessed from a dictionary and letter-to-sound rules.

5.2.10 Virtual Reality

Virtual Reality (VR) is a group of technologies which provide a human user with experiences of artificial worlds which approximate the real world and may enable the user to have effects on objects within the real world. This definition includes many forms of simulation currently used in training as well as *desk-top* VR.

Immersion systems are VR systems that immerse the user in the scenario managed by the computer (with the current state of the technology immersion actually denies some other inputs). Immersion systems may be applied to teleoperation which is the manipulation or direction of effectors from a remote control position. It includes, for example, the operation of remotely piloted submarines and other vehicles. Telepresence is generally taken to refer to the experience of the user in either an immersion or teleoperations system – although telepresence is sometimes used as a term for VR itself.

VR can be divided into systems that use Head Mounted Displays (HMDs) and those that do not. Systems using HMDs are more likely to be immersion-type systems. Desk-top VR, i.e. systems in which scenes/scenarios are viewed through a computer monitor are sometimes excluded from definitions of VR on the grounds that the monitor (the glass) intervenes between the user and the scene. The user, who is then an interactive viewer, is considered unlikely to develop a high level of engagement – a term used to describe the sense of being there.

In virtual realities, the coupling between user and computer becomes much closer than through traditional input and output devices. This is a fundamental change in the way in which we will interact. Head-mounted 3D displays and body sensors like data gloves, data suits or exoskeletons introduce the user into a virtual world in which they can move, perceive and act in close analogy to the real physical environment. The application of VR to C3 is only now being explored but over the next 10 years the potential for it to revolutionise the way in which we interact with complex systems is enormous. Other trends in the area are:

- Training conducted on virtual battle fields;
- Input and feedback devices that incorporate the five senses; and

- Increases in computing power that will enable a richer virtual environment and overcome time lags in feedback.

5.2.11 Artificial Intelligence/Expert Systems

Effective command and control of military systems of increasing technical and organisational complexity requires the application of advanced automated data processing capabilities. Command and control operations are conducted by hierarchical organisations with knowledge, control, authority and resources distributed among the members. The integration of decision-aids into existing organisations requires C3 system technology to be responsive (i.e. near real-time) and of a distributed nature. The application of Artificial Intelligence (AI) offers the potential of optimal utilisation of resources in a time-constrained distributed environment. Two aspects of AI for C3 systems technologies are examined here: real-time expert systems and Distributed AI (DAI).

Expert systems have achieved moderate commercial success, and knowledge-based modelling has allowed the application of decision-aids in domains that have not previously been feasible or practical. However, their application as decision-aids to military operationsl environments still requires technological advances for real-time and distributed use. DAI can contribute in providing representational models for describing and analysing command and control organisations, and the models can be combined with computational tools for the design and integration of decision-aids into existing organisations.

Expert system technology could be useful in four aspects of the command and control cycle: interpretation, prediction, planning, and monitoring. Expert systems offer major advantages due to their intrinsic characteristics of separation of knowledge and control, the natural mapping of the knowledge base into state space search. Research is still required to improve the real-time execution of expert systems. This will include work on problem-solving variance reduction, temporal management, and uncertainty management. The trend will be towards hybrid systems composed of different technologies including, among others, distributed systems, expert systems, and neural networks, in conjunction with traditional mature technologies. The result will be a reduction in time and effort to perform tasks, a reduction of risk, and a more optimal utilisation of resources.

5.2.12 Data Compression Techniques

Currently there is no universally agreed standard for data compression. Any data compression standard can be optimised for the particular type of data, be it video, imagery, English text, or voice. In the military environment, the most pressing requirement for data compression lies in video and imagery. Within the next 12 months, it is likely the US DoD will adopt JPEG (Joint Photographic Experts Group) and MPEG (Moving Picture Experts Group) with minor variations, for image and video data respectively. These commercial standards were developed under the auspices of the ISO committee which first convened in 1987.

These techniques combine to offer compression ratios of between 10:1 (original to encoded) and 50:1 for images, and 50:1 to 200:1 for video. It should be noted that at these ratios the compression is *lossy*, that is, the reconstructed image or video will not be identical to the original. However, when viewed by normal techniques the differences would be minimal. The risk of losing detail, or, potentially worse introducing artefacts into the reproduced product is considered unacceptable in the medical environment and for mission-critical military intelligence. The standard for *lossless* compression is still fluid but the ratios achievable are between 3:1 and certainly no better than 5:1. In regard to text, lossless compression is unlikely to significantly improve on 3:1.

5.2.13 Data/Information Fusion

Data fusion deals with the synergistic combination of information made available by various knowledge sources such as sensors, in order to provide a better understanding of a given scene. As a technology, data fusion is actually the integration and application of many traditional disciplines and new areas of engineering to achieve the fusion of data. These areas include communication and decision theory, epistemology (knowledge science), uncertainty management, estimation theory, digital signal-processing, computer science and artificial intelligence.

While input to a data fusion system consists of sensor data, messages, commands, and prior data, the output from a fusion system represents specific and accurate estimates of the location and identity of a target, entity, activity, or situation. A hierarchy of inferences may be sought depending upon the needs of the system and the levels of representation of the information. The fusion can take place at either the signal, pixel, feature, or symbol level of representation. At the most basic level, the fusion system is intended to determine the existence of an entity or situation. Given the suspected existence of an entity, the next level of inference is the position and velocity of the entity. Closely related to position is the identity of the entity. Higher levels of inference involve the behaviour of entities, and the area of situation and threat assessment. Progressing up in the inference hierarchy requires utilisation of techniques ranging from signal-processing algorithms and statistical estimation methods for combining parametric data, to heuristic methods such as templating, or expert systems for situation assessment and threat analysis.

Artificial Intelligence techniques are appropriate to applications entailing symbol-level representation although some techniques find application at signal, pixel and feature levels. One aspect of the artificial intelligence technology that has strongly dominated data fusion applications is the knowledge-based system. Testbeds already exist to demonstrate this emerging technology. Artificial neural networks provide a fairly robust formalism with which to model the multi-sensor data fusion process. Current research has applied neural networks to pattern recognition and target identification and data fusion for uncertain data and contextual knowledge.

5.2.14 Fratricide Avoidance

While the advances in C3 technologies, for example, the universal use of GPS, should reduce the primary cause of fratricide, there is an enduring need for a tactical-level safety net. Many quick fix IFF (Identification Friend or Foe) devices were rushed into production for the 1991 Gulf War. One example would be the BUDD light – named after its inventor Budd Croley – a match-box-sized IR torch powered by a standard domestic 9 volt dry battery. It emits a low power IR light which is visible through night vision goggles and image intensifiers. In addition to being mounted on vehicles, the unit was small and light enough to be taped to soldiers' helmets. During the crisis, the BUDD light was refined by the Defense Advanced Research Projects Agency (DARPA) (now known under the reduced acronym ARPA) who produced the DARPA light which was much larger, allowed control of the focal plane and was more intense – making it visible from the air. For daytime vehicle recognition, an assortment of techniques were used, ranging from large (0.5m * 1m) brilliant orange and red reflecting panels (known as VS17) to a combination of thermal tapes, some of which were designed to glint in the *near IR* range and others which had low *far IR* emissive properties.

While these quick-fix devices were relatively successful, there remains a requirement for an all-weather IFF system in theatres of operation. There are many technologies which could support such a system. The US-DoD-favoured option is a MMW (Microwave Milli-metric Wave) device currently being developed by McDonnell Douglas, and scheduled to enter service 1996. In the Gulf War 85% of friendly fire incidents were inflicted by the M1A1 tank engaging targets at ranges in excess of 5 Km during conditions when visual identification was difficult or impossible. This proposed system comprises an interrogator which is co-axially mounted with gun systems. Before engaging a target, this device would send out an interrogation signal along the axis of fire. When illuminated, a transponder would return a coded signal identifying it as friendly. A major problem for such systems is making them resistant to deception and exploitation, that is, the interrogator and transponder must transmit an LPI (Low Probability of Intercept) and more importantly LPD (Low Probability of Detection) signal. The proposed system attempts to meet this requirement by the application of low-powered spread-spectrum technology.

This solution can be described as co-operative IFF. The ideal IFF system would rely on non co-operation, and it is likely in the long term this technology will be developed to meet the need for stealth. A non-co-operative IFF system would likely consist of an array of multi-spectral passive sensors and the necessary intelligence to fuse the information and classify targets against a library. These technologies might reduce the problem, but in reality fratricide will remain a product of war.

5.2.15 X.400/X.500

X.400 is an ISO standard and is a full messaging standard. Its binary make up is a header structure and an attached *body part*. The body part may be text or may be any form of digital traffic for example ASCII text for electronic mail, data in communicating applications, ADFORMs, or video.

The document ACP 123 contains details of the military variant of the civil electronic messaging standard X.400. ACP 123 has been adopted by the defence organisation which intends introducing a pilot network in 1994 with full transition from the existing systems in 1998/99. The timetable may be advanced in that AUSTACCS intends to implement secure X.400 in 1995/96 and this may change to a full implementation of ACP 123.

ACP 123 is an evolutionary document and to date the strategic message elements are complete. However there are still gaps in such areas as security, directory services and tactical message handling. Australia intends to design a security policy that will support the entire communication link from writer to reader. Fundamental to the operation of X.400 type messaging is the directory services (X.500). However, there is a conflict that must be overcome in that these directory services must be visible to the world – which is not the traditional way defence does business. X.400 services also pose a cultural hurdle in that it is essentially an interpersonal messaging system, and traditionally Defence works on organisation-to-organisation messaging. At the tactical level where bandwidth is restricted, X.400 may not be the most suitable method of message transfer in that it requires a substantial overhead. Since X.400 supports any type of message traffic, for example, high bandwidth video, intelligent gateways will be required to connect operational-level systems to tactical systems to ensure high bandwidth traffic is not passed on tactical networks causing congestion and potential saturation of networks.

5.2.16 ADFORMS/AIM

ADFORMS stands for Australian Defence FORmatted Message System. It is a system of encoding military-oriented information into structured textual messages and has been mandated for use throughout the ADF. The format is intended to be understandable to human operators and computers. It uses a Murray code set and is based on the NATO ADatP3 and the USMTF standards and is intended to be interoperable with USMTF for a common sub-set of messages.

All ADFORMS messages conform to a basic syntax and consist of a series of *fields* grouped into *sets*. A particular ADFORMS (message type) specifies the sequence of sets required for a message and the sequence of fields within sets. Future versions of ADFORMS will support *conditionality* that is, constraints between different fields and sets.

ADFORMS is currently largely a manual process with computer assistance. AIM (ADFORMS Interface Machinery) is a project to procure software for handling ADFORMS automatically. The software will assist the user in the composition, release, reception, reading and filing of ADFORMS messages. The intention is that the software will run on a stand-alone PC running MS Windows or a SUN Sparc running SunOS. AIM will also provide reusable software modules that can be used in a C3 system to provide ADFORMS message handling.

5.2.17 IMINT Analysis

To date, management of Image Intelligence (IMINT) has been largely a manual process with little computer assistance – the main problem being that individual pixel values cannot be machine-translated into the information content of the interpreted image. Another problem is that the information content is very context dependent and subjective. These are not easy concepts for a computer to process. Management of the products of commercial imaging satellites is recognised as an enormous problem and data management and product distribution issues are being researched actively by many forums.

Shortage of resources to analyse, in a timely manner, intelligence imagery is a very real-time limiter to the usefulness of this medium. The problems of searching a very large area from a great distance cannot be expected to be solved by automatic image interpretation within the time frame of this paper. Progress can be expected in the areas of:

- Automated photogrammetry; and
- Change detection where the changes to be determined are specific and there is a lot of collateral information about the scene.

5.3 Communications

5.3.1 Main Directions

Future communications systems will be based on developments currently taking place in three, primarily distinct technology areas:

- ATM (Asynchronous Transfer Mode);
- New protocols; and
- Global networking.

The developments in these three areas have already begun to produce a synergism of technological advances in communications. Other technology areas such as data compression, fibre optics, and Multi-Level Security will also contribute to these advances.

5.3.1.1 ATM

Asynchronous Transfer Mode (ATM) networks are clearly on the horizon as the next generation networking technology, and it is expected that ATM will be "the fastest-growing segment of communications" technology during the remainder of this decade (IEEE Spectrum, January 1994). Unlike previous technologies which were designed to support primarily one form of communication, ATM networks are the communications focal point for the convergence of voice, video, and data.

ATM is a switching and multiplexing technology and is the fundamental building block of Broadband Integrated Services Digital Network (B-ISDN). B-ISDN is the standard for the next generation of global communications and at current market projections will be in general service before the end of the decade.

Although conceived by the telecommunication carriers, the ATM protocol can support the coming generation of high-bandwidth traffic, be it video, high-resolution colour imagery, voice or distributed computing. ATM is expected to be the standard for the next generation of computer networking. ATM computer networking products are beginning to appear on the commercial market. However, the current range of products are expensive and are aimed at the specialist market, i.e. where extremely high bandwidths are required. Within the next 18 months the price of ATM products is expected to fall resulting in more cost-effective high-bandwidth computer-networking than established alternatives such as Fibre Distributed Data Interface (FDDI).

ATM offers many benefits which include:

- The ability to integrate all forms of digital traffic, i.e. voice, message, computer data and video. This is a complex engineering task since this traffic is a mix of isochronous (real-time), stream (constant bit-rate), and *bursty* (variable bit-rate) data and each service has a different tolerance to propagation delay and cell loss.
- Very high bandwidth and a fully scalable standard with no theoretical upper limit. The standards for 155 Mb and 622 Mb per second are established and it is expected 2.4 Gb and 9.6 Gb per second will be agreed in the near future.

- Support of statistical multiplexing. One of the problems for all data networks is that the exchange of computer data tends to be very *bursty* in nature, that is, the communications network may be required to service a very high peak instantaneous demand but then sit idle for many seconds. As a consequence, the average demand is relatively low. Traditionally, in the days of leased-lines, external data connections were dimensioned for the peak loads. This is obviously wasteful during the periods of low activity. Statistical multiplexing offers the alternative of aggregating many computer connections such that carrier bandwidth may be little more than the sum of the average demand, thus making efficient use of bandwidth. This requires complex analysis of the component services and dimensioning the network such that there is an acceptably low probability that users would exceed the bandwidth allocation. ATM is not unique in supporting statistical multiplexing – other modern data transmission standards also support this feature, for example, Frame Relay.

The ATM standard requires that digital information is segmented into small (48 Bytes) fixed length payloads without any error detection information and attached is a 5-byte header to form a 53 byte cell. The 5-byte header contains information which identifies the payload uniquely. The identification process is at two levels: first, end-to-end across the network – referred to as Virtual Path Indicator (VPI); and second, by the actual service to which the payload belongs, referred to as the Virtual Channel Indicator (VCI). In addition the header contains information relating to the quality of service required by the payload (pay-load type identifier and cell loss priority) and error correction information which can detect and correct single errors within the header.

Many technical points can be drawn from the above overview of ATM, the more important being:

- First, the small fixed length packets, referred to as cells, give ATM the flexibility to deal with real-time traffic – examples of real-time traffic being voice and video, i.e. these services rapidly degrade if random duration delays in transmission are introduced.

- Second, no error detection information is included in the payload. Any error detection codes are an overhead and reduce the effective throughput of the system. The rationale of not building error correction into the payload is that modern fibre optic connections have such low error rates (now approaching one bit in 10^{12}) the likelihood of corruption is almost negligible.

- Third, the small five byte header is very simple and is designed such that all switching can be done using hardware. Hardware switching is very fast in comparison to protocols which require software algorithms for switching. Hardware switching therefore reduces the delay of information through the network (propagation delay).

Militarising ATM

ATM is a commercial standard and has many features not optimised for the military environment examples being billing mechanisms and fraud control measures. ATM does not have many features which are critical in military systems examples being information and traffic security features and the ability to pre-empt low-priority users. Military communications have fundamental philosophies. For example if bandwidth became limited on a network servicing many video channels, decisions would have to be made about limiting services. The military user would be prepared to tolerate a very high degree of distortion, accepting that in a crisis situation something is much better than nothing, i.e. the same number of channels but a lower quality. On the other hand, the civilian user would not want anything less than full quality and the answer would lie in disconnecting some channels in order that others could remain full quality.

ATM is designed for very low error-rate fibre networks. In the military environment where mobility is critical at the tactical level, satellite and beyond line-of-site radio systems would be used as the bearer medium. Such systems generally suffer from fading and significant noise which can give rise to high error rates. To make ATM cells more survivable, in particular the header information has to be made more robust. Options include modifying the standard by changing the internal of the header or adding additional information to the ATM cell.

ATM offers the greatest benefits in integrating a large number of high-bandwidth services. Since ATM is a commercial standard, the development effort is focused at the very high speeds, i.e. 155 Mb/s and above. However, in the military, communications links to the tactical commander are for the foreseeable future likely to be essentially narrow band. Research and development of low data-rate ATM standards are likely to have to come from within the military.

Research under the US Air Force's Secure Survivable Communications Network (SSCN) program and DSTO's DORIC (Defence ORganisation Integrated Communications) program, is being conducted into integration of ATM signalling with advanced satellite communications capabilities. The general concept is to ensure that advanced communications switching capabilities being developed via ATM will be interfaceable and globally extendable using satellite networking technology. The experimental evaluation will initially investigate the problem of moving data more efficiently through the relatively narrow band (1 to 2 Mb/s) bandwidths associated with mobile tactical systems. SSCN will also address the ability to interconnect high data-rate nodes through relatively narrow band line-of-sight radio and satellite links more efficiently by adaptive bandwidth control using ATM protocols. Combined voice, video, data and image transmissions in ATM format within a 1 to 2 Mb/s bandwidth are of particular interest. Eventual experimentation will interface the ATM signalling rates of 155Mbs with the satellite links.

5.3.1.2 New Protocols

With the rapid growth of global communications systems and the transition to new networking technology such as ATM, it has become clear that existing protocols for information transfer through these systems are not adequate. The tremendous growth (15% per month) in the number of sites, hosts, and users of the Internet has reduced the effectiveness of protocols designed for a much smaller network. New addressing methods, such as variable bit-length addresses and new routing protocols must be developed to operate at the data rates supported by ATM. These will include the low-level protocols for routing, traffic, and error control, as well as the higher level protocols for establishing connections and application-level protocols to support multi-media communications. In a global environment with military applications which must span not only the high-speed ATM backbone network, but also extend into lower bandwidth networks reaching down to a remote command post and even to the individual user, protocols must be designed to recognise and adjust dynamically to the current network configuration and traffic patterns.

5.3.1.3 Global Networks

Advances in networking technology will also play a major.role in influencing the direction of communications technology development. The growth of a truly global network infrastructure serving civilian/commercial users provides a significant resource for military communications systems. The civilian/commercial networks will be expanding worldwide much faster than military systems can be expected to do alone. Thus it will be important for defence organisations to be able to utilise these resources on demand. As ATM networks become available in both military and civilian systems, such on-demand access will be possible. For example, using ATM networks with distributed network control, it will be possible to establish, on demand, a virtual private network with a specified capacity, latency, and security. This level of dynamic control, coupled with the inherent redundancy in the combined global civilian/commercial networks and military networks will provide much greater survivability and reliability than current military systems alone. In order to capitalise fully on these resources, all military applications must be able to utilise these networks and thus must be fully interconnected. This will represent a significant challenge for the development of multi-level secure networks. Advances in fibre optics, such as the use of distributed fibre amplifiers, will continue to enhance high-bandwidth networks by providing fibres directly to almost every user.

ATM lends itself to the principle of Virtual Private Networks (VPN). Within any communications network, be it commercial or military owned, bandwidth can be reserved for particular users or groups of users, establishing a VPN. The actual traffic passed, provided it does not exceed its bandwidth reservation, is solely a matter for the VPN operator, not the network owner. In many ways a VPN is modern day equivalent to leased lines with the important difference that VPNs are configured in software and hence can be dynamically allocated.

The civil telecommunications providers have embraced and are actively researching the concept of Universal Personal Communication (UPC). The aim is for a subscriber to have global access to the telecommunications network via a light-weight cordless terminal. A subscriber anywhere in the world will be able to access, and be accessed by, services through a Personal Telecommunications Number (PTN). To support such concepts, Intelligent Networks (IN) will be required which are able to locate, authorise and bill users. While noting that the military impact of such technology in the medium term is minimal, ultimately it will become cost-effective to equip all military personnel with UPC devices. However, such a policy would imply a significant increase in the number of users in the military communication arena and would require an enormous increase in communication infrastructure, particularly at the tactical level.

5.3.2 Support to the Mobile Commander

It is generally recognised that communications to the mobile commander are going to be bandwidth-limited. The interface between the fixed high-bandwidth systems and tactical mobile systems is a potential information bottleneck.

Although ATM is a broadband technology and largely inappropriate to narrow band HF systems, many of the features of ATM hold potential to be adapted to optimise throughput on narrow band channels. An example would be ATM's ability to multiplex traffic types which require different qualities of service, e.g. multiplexing voice and data in a single HF channel.

5.3.2.1 HF Radio

The traditional bearer for beyond line-of-sight communications to the Mobile Commander is HF radio. Radio waves at these frequencies are reflected, or more correctly refracted, by the ionosphere, a region of the upper atmosphere which is between 80 and 300 km above the earth's surface. The refractive index of this region is proportional to the free-electron density which in turn is affected by radiation from the sun. Although the sun's activity is broadly predictable, many solar events occur at unexpected times with little or no warning. Such events can on occasions enhance HF radio wave propagation beyond predicted levels or modify the ionosphere such that all HF radio waves are absorbed and no propagation occurs at all. Such extreme effects can last from seconds up to several days.

Within the next 15 years it is not feasible to conceive of a man-made ionosphere which could be used to replace or supplement the natural ionosphere. However, some theoretical physicists have suggested that this may be possible.

HF communications is limited to relatively narrow bandwidths. Current modern HF modems can support digital data rates of 2.4 Kb/s with average HF propagation conditions. Current HF modem research, under the auspices of the DORIC program, is targeting data rates of 10 Kb/s. These modems rely on a non-invasive real-time channel estimator driving a feedback loop to the transmitter which adaptively varies the data rate to suit the instantaneous conditions. In such a system, if conditions reach the top of a fading cycle, the data rate would be very high, while if conditions were very poor, it would cease transmitting and wait until they improve. There are several intermediate data rates between these extremes. In this way it is expected to achieve an average of 10 Kb/s with an error rate of 10^{-4} over an average HF channel.

5.3.2.2 Satellite communications

INMILSAT

The INternational MILitary SATellite (INMILSAT) program provides a good example of current trends in satellite communications systems. Initiated by the near-future block-obsolescence of US, UK and French satellite communications assets, a multi-national system is being pursued. The Space & Missile Centre (SMC) of the US Air Force Material Command (AFMC) is currently conducting a multi-contractor study to investigate the issues of developing such a system and is proposing various standards, satellite architectures, and spacecraft and payload configurations for the satellite system.

The baseline assumption is that the communications payload will focus mainly on SHF (Super High Frequency) capability with the possibility of a modest amount of Low Data Rate (LDR) EHF (Extremely High Frequency) capability. Some of the primary goals for the satellite system are:

- Enhanced support for higher data rates into small, mobile terminals;
- Increased responsiveness to the tactical user; and
- Simultaneous optimisation of the space and ground segments to minimise life cycle costs and to enhance user performance.

Payload design issues include the choice between on-board processing capability versus bent-pipe repeaters. On-board processing has the penalty of increased complexity for the payload but the advantage of increased performance for the users through reduced system noise and more efficient use of the spectrum. One of the key processing approaches to be studied includes the use of an on-board universal modem. This modem would have the ability to demodulate and modulate a variety of waveforms. This feature makes the design control for the ground/airborne terminal segment much easier to address.

Control of the system in general must address the issue of centralised versus theatre-based payload control. Additionally, the use of cross-links between satellites must also be assessed. Satellites could be manufactured individually by each country with the cross-link hardware being held to some standard waveform and performance criteria. This would allow for independent designs for up and down-links, with communications between differing forces being provided via the cross-links. The allocation of resources within the architecture must also be addressed.

Satellite Technology Trends
The key technology area for any payload design is the up and down-link antennas implemented on the spacecraft.

The desire to communicate at high data-rates with small terminals is a primary goal for future tactical forces. Typically, the limiting factor in the accomplishment of this goal is the power available from the spacecraft down-link antenna. The first factor to be considered is the practical limits of the power available from the spacecraft. Spacecraft sizing for INMILSAT must be compatible with the ability to launch with a Medium Launch Vehicle (MLV). This limits the power available. However, advances over the past 5 years have enabled the realisation of increased power available to the payload from reasonably sized spacecraft.

The next area of concern is the efficient generation of Radio Frequency (RF) power. Several designs can be considered, but the most elegant design is an active-transmit phased array. Transmit phased arrays can be tailored on-orbit to address varying theatre sizes and shapes. Power is efficiently combined via spatial combining. Graceful degradation of the down-link performance is also provided through the use of many elements, each of which provides power. The performance degrades as a function of modules eventually failing over time.

Designs which incorporate multiple Beam Forming Networks (BFN) within the design are also an evolving design possibility. This will allow for the realisation of several beams from the same aperture. This represents a huge cost and weight saving for the spacecraft. The flexibility of the system also grows. Multiple BFN designs can be realised for the up-link antennas. Up-link antennas on the space craft for military communications must address adaptive nulling capabilities to minimise the effects of ground-based jammer terminals. The ability to perform this nulling in an automated fashion without ground control is desirable and much work has been accomplished in this area. The up-link antenna design of choice typically includes agile beam Multiple Beam Antennas (MBA) with off-set reflectors or lens design approaches. The exact choice depends on the system goals and desired performance. To support communications for a user who is geographically close to an enemy jammer (50 kms), a high degree of resolution is needed from the spacecraft up-link antenna. Typical approaches for the INMILSAT system will include the use of distributed apertures mounted on extended booms. These antennas are then phased together to perform high-resolution nulls.

Improved performance for the spacecraft up-link is a goal of the future – to support communications to smaller terminals. This mainly addresses increased antenna gains (wider apertures) with a smaller contribution coming from improvements gained from more sensitive receivers.

There are currently at least six commercial proposals being touted for Low Earth Orbit (LEO) satellite-based global communication systems. These systems are essentially narrow-band systems supporting of the order of 10 Kb/s from hand-held devices. An example would be the Motorola Iridium proposal which was originally conceived to consist of 77 (the atomic number of the element Iridium) active satellites arranged in 7 polar orbits. It is due to be in service in 1997 with a market projection of 1.8 million customers in the initial period of service. The project costs are estimated at US$3.1 billion.

5.3.2.3 Tropospheric scatter

The troposphere is the lowest region of the earth's atmosphere and extends from ground level to a maximum height of 10 kms. All cloud formations and weather occurs in this region. The troposphere is a turbulent collection of air masses at different temperatures with many vortices and eddies. In addition, there is laminar motion of air masses. The boundaries to these different air masses form discontinuities and electromagnetic waves experience a scattering effect as they transgress each boundary. Hence tropospheric scatter can be exploited as a mode of radio wave propagation if a transmitter and receiver can *view* a common volume of troposphere. The path loss of such propagation is extreme and normally associated with deep fading. Typical losses are between 190 and 240 dB. (Note a typical line-of-sight radio link has a path loss of 120 dB). Curvature of the earth limits the maximum range of such a mode of propagation to approximately 1,000km. However, 300km and 150 km is generally the maximum distance for fixed and mobile systems respectively because the lower troposphere is more efficient at scattering.

Due to extreme path losses, traditional tropospheric scatter systems consist of high-powered transmitters, high-gain (large) aerials and very sensitive receivers. However, by exploiting space, volume and frequency diversity with advanced signal-processing and high-efficiency transmitters and low noise receivers, the bulk of tropospheric scatter systems is reducing while the range and bandwidth are improving. There are transportable systems commercially available which offer data rates of 512Kb/s at ranges of up to 100 km. Such systems tend to use SHF with medium power transmitters (100W) and self-aligning dish aerials of the order of 60 cm diameter.

Phase 7 of project PARAKEET, the trunk communications which will support AUSTACCS (Australian Tactical Command and Control System) is acquisition of tropospheric scatter equipment. However, this phase has not been approved.

5.3.2.4 Multi-band Multi-function Radio

There is growing support within TTCP member nations for the development of a multi-band multi-function radio. The radio will support data and voice communications and is backward compatible with most existing UHF,VHF and HF radio systems. The design is modular, meaning that a core set of modules will provide a basic communications capability, while adding additional modules will extend performance. In other words the radio will support man-pack, vehicular, shelter and ship-borne requirements. These diverse applications are handled through addition of core module sets to meet the specific operational requirements. The US led radio design is based on digital processing and the software is written in Ada. Future enhancements will be accomplished totally in software keeping pace with changes in operational requirements. The radio is designed with joint force, service interoperability in mind. The current design includes the ability to add satellite communications in the future with the addition of high transmit/receive modules. Due to its common modular design, the radio will bring a whole new concept of field maintenance to the operational community due to just the economy of scale factor alone. Maintenance will be achieved with fewer module spares and with fewer field maintenance personnel. The radio design provides an enormous step toward satisfying communications interoperability requirements for multi-national operations.

5.3.3 Survivability Risk Analysis

The Defence Corporate Communications Plan (DCCP) clearly states the Government's policy of directing the Defence Organisation to make maximum use of civil infrastructure, standards and equipment. The economic rationale for this policy direction is immediately obvious. However, this policy does raise the issue of survivability, i.e. how survivable is the civil communications infrastructure? To assist Defence network planners, under the DORIC program, DSTO has developed a survivability risk analysis method which is customised for analysis of civilian telecommunications infrastructure from a military viewpoint. This methodology was demonstrated recently when it was applied to part of the Telecom Australia's PSTN. It has specific capabilities:

- It allows high-level and strategic views of civil communications networks which may be extremely complex;
- It combines both static and dynamic analysis as it addresses both the susceptibility of assets and the impact of the loss of the assets;
- It incorporates Defence criteria on physical security, information security and trusted computer systems;
- It provides graduated assurance scales for counter measures to logical threats by means of the ITSEC (Information Technology Security Evaluation Criteria); and
- It allows other risk methodologies to be added for specific situations, for example contingency planning.

With the current policy of making maximum use of civil infrastructure where appropriate, such methodologies are essential if informed and balanced decisions are to be made.

5.4 Sensors

5.4.1 IR Sensors

Night vision devices, be they goggles, weapon sights or drivers'/pilots' navigation aids, are based on one of two technologies, that is, either image intensification (discussed later) or thermal imaging also frequently called FLIR (Forward Looking IR). FLIR sensors work by converting environmental temperature differences, that is far IR in the 8 to 14 um wavelength region into electrical signals. First generation devices use scanning mirrors to produce a monochrome raster picture. Second generation FLIRs are being developed which detect the near IR 3 – 5 um wavelengths using Focal Plane Arrays (FPA) and advanced cooling systems. Such devices are smaller and lighter primarily due to the reduced cooling requirements to detect the shorter wavelengths – they operate at the warmer temperature of 175K as opposed to first generation at 77K. Many of the latest generation personal devices are stabilised to operate at room temperature. Prototypes of a second generation device have been fielded as weapon sights weighing less than two kilos. These devices are expected to be cheaper and very importantly for the tactical arena, quieter. Another advance is that the next generation will produce a red and black image, as apposed to existing systems which produce green and black. Red images are considered more compatible with a human's own night vision. More significantly this generation of IR sight can produce a TV standard output which is easier to integrate into a wider C3 system, rather than just being a personal vision device.

IR sensors have a valuable role to play in the tactical area in that they have an ability, albeit limited, to penetrate poor weather and smoke. During the Gulf War, ground forces used IR sensors for target identification at short range since this was frequently found better than via visual means. However, IR sensors are essentially short-range devices and although target detection may be possible, even with the next generation of sensors, target identification at extended ranges will remain difficult with these type of sensors alone.

5.4.2 Visual Imaging

Within the next fifteen years visual imaging is most likely to be the richest medium for gleaning intelligence. The resolution of any sensor is limited by the wavelength of the bearer medium, but in the case of visual imagery from a military perspective the nanometric wavelength offers unlimited resolution. The fundamentals that sight is the highest bandwidth human sensor, and that humans possess highly developed visual processing abilities, combine to make visual imagery a powerful medium for transferring information. Optics is a mature technology and photo-electronic detectors are relatively simple, cheap and compact devices. The major limitations of such sensors are the level of illumination required and obscuration caused by atmospheric conditions. While the former limitation can be offset by increasing the aperture of the sensor, all visual sensors will be at the mercy of the weather.

The greatest practical coverage area is achieved by mounting an optical sensor on a geostationary satellite. Such a device could view approximately 40% of the Earth's surface. To achieve 10 metre resolution from an optical sensor on such a satellite, that is, at a distance of 36,000 km from Earth, a telescope with a minimum of 5m diameter is required with average daylight conditions. However a single aperture 5m telescope, while being technically feasible would be prohibitively expensive to manufacture and launch. To illustrate this point, the NASA Hubble Telescope is a state-of-the-art 2.4 metre telescope which cost over US$2 billion. To compound the problem, the cost of a space-mounted telescope is proportional to the sixth power of the telescope's diameter. Hence, a five metre telescope is likely to cost of the order of $64 billion. There are two basic solutions to reduce this cost. The first option is to develop multiple small aperture telescopes which could be combined to synthesise a large single-aperture device. Such devices are not currently available but are theoretically possible and may be developed within the next decade. The other option is to reduce the operating distance of the sensor.

High and low earth-orbit satellites operate between 1000 km and 300 km above the Earth's surface. For such a satellite to achieve global coverage it would have to be in polar or near polar orbit. In general terms such satellites pass over all areas of the Earth's surface once in daylight every 24 hours. A modification of this type of platform is for the satellite to have some form of propulsion system such that the orbit of the satellite could be modified to cover an area of interest. A problem occurs in that comparatively large amounts of energy are needed to modify satellite orbits. Since nuclear devices in space are politically unacceptable, and current solar technology cannot provide adequate power, the only viable option for providing this power is chemical-based propellants. This in turn presents options of launching the satellite with adequate propellant for its operational life, perhaps up to several 10 tonnes of propellant, or having some form of in-orbit re-fuelling. Both of these options have prohibitive cost overheads.

From an ADF perspective the ADMI is in global terms relatively small in area and fortuitously geographically close to the equator. These facts give rise to the possibility of placing a low earth-orbit satellite in equatorial or near-equatorial orbit which would cover a large proportion of the ADMI once every 90 minutes. At current prices, a visual surveillance satellite to cover the ADMI has been estimated to cost of the order of $1 billion. This magnitude of cost is broadly comparable with the cost of the JORN.[1] However, with advances in miniaturisation of electronics and increasing availability of launch platforms, the cost of manufacturing and launching satellites is likely to continue

[1] Comparison of JORN and satellite surveillance is a complex issue and an important consideration is that current satellite based sensors cannot reliably detect and track aircraft. On the other hand JORN is a doppler radar and has a high probability of detecting fast moving aircraft.

to fall increasing the ADF case for satellites as a cost-effective wide-area surveillance tool. In April 1992 the AFCEA (Armed Forces Communications and Electronics Association) issued a report which determined the cost of building and launching a reconnaissance satellite with a 2.5 metre resolution (about that required to pick up an individual vehicle) would fall to $60 million within the next few years.

To operate visual surveillance satellites efficiently, real-time monitoring and prediction of the weather is a key requirement. Operators must be able to predict cloud movement and be able to assess which areas of interest will be visible during a satellite's pass. Having made these deductions, for maximum efficiency they must also be able to control pointing of the camera in real-time.

The final option for reducing the operating height of the visual sensor is to mount it on an aircraft. This has the obvious limitations of comparatively reduced area of coverage, i.e. the area of coverage is proportional to the square of the height. Other aspects to be considered are political issues of ownership of airspace, ease of detection (and hence avoidance), and vulnerability of the platform. A variation that is potentially useful in the ADMI is long focal-length lenses mounted on aircraft which could patrol in international airspace. Such an arrangement could give useful visual intelligence 50 miles inland. Therefore such an arrangement has significant potential for intelligence gathering of island land masses.

Image intensifiers are a mature technology which first appeared in 1950. They work by amplifying ambient light, normally from the moon and stars by focussing photons on a photo cathode which in turn releases electrons. These electrons are then accelerated and projected onto a phosphor screen. Current third generation image intensifiers offer a high resolution, cheap and very light-weight (less than half a kilo) aid for night vision and offer a cost-effective means of improving situation awareness in the tactical arena.

One of the richest forms of intelligence to a C3 system lies in IMINT. The availability of high resolution imagery in the near future is likely to increase with developments by commercial ventures such as SPOT and the commercialisation of spy satellite technology. Such developments are expected to provide 1 m resolution imagery within a few years. With the dramatic fall in cost of satellite technology, many commercial ventures are investigating the market for providing national space-imaging sets. As well as space assets, tactical aircraft and UAVs (Unmanned Aerial Vehicle) are likely to be used to provide real-time image intelligence.

5.4.3 Radar

Radar has an enduring role at all levels of the military environment principally due to its all-weather capability. However, the wavelengths used in radar limit the bandwidth of any practical system to the order of 300MHz, which is eight orders less than a visual system. As well, radar images are relatively difficult to interpret because the intensity of reflections bear little relation to physical size but are highly dependent on corners and to a lesser degree straight edges. To illustrate this difficulty, current state-of-the-art systems can analyse radar data in approximately one tenth real-time.

5.4.3.1 INGARA

In March 1993 DSTO conducted airborne testing of their synthetic aperture radar known as INGARA (formerly AuSAR). The basis of Synthetic Aperture Radar (SAR) is to synthesis a radar with a large high-gain aerial which could offer very high angular resolution with, in reality a small light-weight antenna. The complexity of the system is in the signal-processing required to achieve this aim. The technique is to build up a series of low resolution images all taken from slightly different vantage points. SAR are directly relevant to airborne operations where size and weight are major constraints.

The mode of operation is for the SAR-equipped aircraft to fly in a straight line at a constant altitude, approximately 3,300 metres and survey a swath out to the side of the flight path at a stand-off distance of approximately 25 km. The resolution of SAR is independent of height but dictated by the width of strip to be surveyed. Typically for a 12 km swath the resolution would be approximately 3 metres which provides enough resolution to detect ground vehicles and small boats.

The INGARA is a cost-effective remote all-weather sensor. In addition to performing wide area surveillance for the ADF, the INGARA could be used for commercial applications such as land management, environmental monitoring and bush-fire monitoring. To date, the demonstrator project has cost $5m. Costs have been kept down using COTS hardware and software where possible. The current model records a tape for ground analysis, but future development will include a real-time processing capability.

5.4.3.2 JORN

The Jindalee Operational Radar Network (JORN) will be a network of two north-looking over-the-horizon radars, one in northern Queensland, Longreach (90 degree view) and the other in Western Australia, Laverton (180 degree view). This network is due to be operational in 1997. Towards the end of this decade a decision will be made on whether to enlarge the network to include a central radar. The radar sites will be connected via broad-band communications links to a Joint Coordination Centre (JCC) in South Australia. Radar tasking, data fusion and network management will be controlled at the JCC.

JORN is based on the Jindalee Over-The-Horizon-Radar (OTHR) which was developed and demonstrated by DSTO using the JFAS (Jindalee Facility Alice Springs).

The concept of OTHR is based on transmitting a continuous wave frequency-modulated HF radio signal which reflects from the ionosphere onto the target. A minute quantity of energy is reflected by the target and returned via the ionosphere to a receiver site. The majority of energy transmitted will be returned by the ground or sea and therefore doppler shift is used to detect the target. Hence OTHR can only detect a target moving with a radial velocity component relative to the receive site. OTHR has a high probability of detecting fast-moving aircraft and under favourable ionospheric conditions will be able to detect slow-moving ships.

The major limiting factor in performance of OTHR is the ionosphere which is a dynamic and, in many ways, a fickle fact of nature. Typical range accuracies for OTHR are of the order of 40km and bearing accuracies of the order of 0.5 degree. However, many techniques can be used to improve these figures. One of the simplest is the use of HF transponders in accurately-known positions. This principal could be expanded to a HF-type of IFF system which could be operated by co-operative units. It is possible to exploit information from co-operative civil aircraft. For example, the Future Air Navigation System (FANS) which will be used by large civil aircraft, continuously transmits the position, height, speed, direction and coming way points, all via satellite, to a centralised air control centre. Fusing this data with JORN positional information could improve co-ordinate registration – and hence accuracy. Other advances to JORN will rely on improved signal processing techniques which could improve system performance particularly under adverse ionospheric conditions. The current system requires highly skilled operators. Expert Systems hold potential to ease operator load and increase the efficiency of the system.

5.4.4 Bi/Multi sensors

No one sensor is ideal for all conditions. To answer to improving sensitivity and accuracy in the near term is to use multiple sensors and to fuse the incoming data into a single reliable picture. Advances in technology are making individual sensors smaller and lighter. Greater processing power is also becoming available. Hence multi-sensors are a natural evolution.

Examples in the battlefield would be radar combined with IR; for wide area surveillance, SAR and visual imaging; and for high altitude surveillance, IR with visual imaging.

This page intentionally left blank

SECTION 6
CONCLUSIONS

6.1 General

The next 15 years will be a period of rapid change for C3 systems. The time between significant advances in hardware and software will continue to decrease. Current IT systems are often obsolete within three years. Future C3 systems must be allowed to evolve continuously if they are going to take advantage of technology advances and maintain a technological superiority. It is envisaged that the infrastructure for future C3 systems will be largely based on Commercial-Off-The-Shelf (COTS) products. This infrastructure may offer a richer functionality than strictly required for military purposes and will host special-to-battlefield functions as required. The open COTS product market will also enable a potential adversary to exploit such products in threat systems. Hence there should be a shift from the goal of purely a *technology superiority*. The challenge in an open COTS market is to develop smart applications supported by this advanced technology to strive for a *capability superiority*.

6.2 Key Requirements of Future C3 Systems

Modern joint warfare concepts mandate the need for an integrated Navy, Army, Air Force unified command. The ADF will be expected to be able to work closely with many other Government organisations and allies. Interoperability will be a key issue in enabling such diverse organisations to work together. The corner-stone of achieving interoperability will be standards. However, acquiring systems which meet the right standards is an extremely complex issue in view of the general lag of standards behind technological advances and the almost transient nature of standards. Hence, standards will be a challenge for C3 systems for the foreseeable future.

Technologies are emerging which will enable: applications to be constructed, run and maintained on multiple dissimilar platforms; and object-based applications to be constructed, run and changed on multiple platforms. The key technologies are Middleware and Distributed Object Management. OSF's (Open System Foundation) DCE (Distributed Computing Environment) is an emerging middleware standard on which many products are based. It will provide cross-platform interoperability so that information and processes can be shared by platforms of a dissimilar nature. Distributed Object Management will permit distributed application integration. The OMG's (Object Management Group) CORBA (Common Object Request Broker Architecture) specifies the criteria for distributed object management. It will enable applications to be constructed easily and will make use of the platform interoperability provided by DCE.

The most basic requirement will be for interoperable communication systems. ATM (Asynchronous Transfer Mode) is the switching technology which is the basis of B-ISDN (Broadband-Integrated Services Digital Network). B-ISDN will be used for global civil communications before the end of this decade. It is logical that the military should also adopt this standard. However, because B-ISDN has a commercial pedigree, it will require some militarisation. Co-ordination of the militarisation of the ATM standard will be an essential but politically difficult task which must be achieved as a fundamental building block to multi-national interoperability.

A commander's understanding of a situation is fundamental to his ability to plan, react and make good decisions. Therefore a fundamental requirement of a C3 system is to provide a full and accurate situation display. For effective operations, this common picture must be shared at all levels of the organisation and, if part of multi-national operations, by all national commanders. As with many C3 issues, although a technically difficult challenge, the ultimate limitation will be at the organisational and political levels.

6.3 Security

A limiting issue that will dictate the interoperability achievable among C3 systems in the next 10-15 years will be communications and computer security. The situation is becoming more complex with the introduction of greater connectivity and distributed systems. MLS (Multi-Level Security) is part of the answer and although vendors claim products to support MLS are just on the horizon, the US C4I for the Warrior program does not envisage full MLS operation until 2010. Incremental solutions, however, are available. While there are problems with existing MLS systems (e.g. administration, audit, user-interfaces, etc.), the R&D community is working on efforts to enhance the capabilities and performance of MLS products.

Challenges will arise when multi-national MLS systems are to be inter-connected. Unless all systems are considered to afford the same level of trust by all, then information sharing will fall to the lowest common denominator of security classification. Joint certification of levels of trust of national systems will be a time-consuming and politically complex task.

With the growing dependence on IT-based C3 systems for effective military operations, these systems will be an attractive target to any enemy who may attack either physically or computer-based (logically). Measures must be taken to protect against such attacks and, in particular, overall system design must avoid a single point-of-failure that could disable the entire system.

6.4 C3 System Procurement

The current approval process for C3 system procurements is based on the waterfall method where project requirements are specified up-front, systems are procured and maintained for their useful life before finally being disposed of. It will require a significant change in culture to accept that a system will be permitted to evolve and grow over time. Evolutionary Acquisition (EA) is a project management process which supports incremental acquisition and which can significantly reduce a project's exposure to cost, schedule and technical risks. However, one thing EA cannot do is specify the total costs at the beginning of the project. Therefore EA presents a challenge within the current approval process. Although there are currently two major projects in the initial phases of acquisition which are embracing many of the principles of EA, more work needs to be done to assist in its wider acceptance by procurement authorities.

In view of the uncertainties in future conflict settings, the identification of user requirements for C3 systems to support command and control is consequently speculative. However, experience and recent evidence suggests that an infrastructure embodying a core functionality can be defined and that this infrastructure can host a useful range of applications. Rapid prototyping using this infrastructure and the advanced development environments now becoming available should decrease the cost of this activity. While the infrastructure approach should provide important stability in the procurement process and facilitate the development of user requirements (e.g. by rapid prototyping in the application layer), problems in system testing and acceptance are likely to remain.

Traditionally the intelligence community has worked behind closed doors. Intelligence collection, analysis techniques, information processing and distribution systems - due to their sensitivity, all are veiled in secrecy. There is growing recognition that intelligence system requirements are in many ways similar to C3 systems requirements and hence many of the technologies required to support them are the same. Therefore future procurement of support for C3 and intelligence systems should exploit commonality and avoid duplicated effort.

The coming generation of C3 system users are more likely to be computer-literate. There are two areas that can exploit this resource. First, future C3 systems should engage the computer-smart user in the procurement process. Not only should this engagement assist in procuring a better product but also lead to greater sense of ownership and hence system acceptance by the user. Second, future C3 systems should have facilities to support user developed software. User developed software goes beyond allowing the user to customise an interface but allows generation of high level code to optimise use of a system. However, a note of caution if user developed software is supported, the commander must retain control to manage the degree to which the user may influence the system to ensure overall performance is not impaired.

6.5 Communications and Networking

Communications networks are increasing in complexity and scope. They are providing a diversity of services, growing in capacity and are incorporating increased intelligence. These trends are increasing the risk of network failure arising from either errors in the design of the network software or from deliberate attack. In addition, the consequences of the failure on the network's users is likely to be more severe than in the past. At high transmission rates, networks will become large buffers which can easily become congested unless something is done to control this data latency. Network behaviour, both under normal conditions and under stress, is becoming more difficult to understand and even more difficult to predict. In particular, prediction of peak transient conditions will be vital. The current difficulties in the management, accurate modelling, and simulation of networks will be much greater with the new networks. In future conflict, military networks will rely greatly on existing commercial infrastructure and as a result, there will be increased problems concerning security control of network resources.

Future C3 systems will be based on multi-media and distributed computing technologies. In order to function in a timely manner, these technologies must be supported by high bandwidth communications. An ideal C3 system would have the same architecture from high-level strategic areas to the lowest-level tactical fighting unit. Fixed optical fibre holds the potential for virtually unlimited bandwidth but beyond line-of-site communications to support the Mobile Commander will be either narrow band or extremely expensive. The problem may be mitigated by advances in HF modems (to improve throughput), cheaper more-mobile tropospheric scatter, satellite communications systems, more efficient traffic management, multiplexing techniques and compression algorithms. In reality, however, communications bandwidth at the tactical level is going to be a limited and precious resource. Hence the operational/tactical interface has the potential to become an information bottleneck.

Network management and administration of future distributed systems will be a formidable technical challenge. Even basic issues such as software updates, fault isolation, work-around and recovery of geographically dispersed systems will be problematic. Unless progress is made in resolving some of these relatively mundane issues, future C3 systems are likely to be little more than pipe-dreams and unusable in the real world.

6.6 Decision-Support

COTS products are just beginning to emerge which address collaborative and group working. To date, IT-assisted planning and decision-making in the C3 environment has been performed by users working independently. Now products such as Lotus Notes are allowing group preparation of planning documents. There is likely to be a proliferation of COTS group-ware products in the coming years. To be fully interoperable in a joint and multi-national environment, these common products should be adopted. Another related challenge will be translating existing planning aids from single-user environments into multi-user systems.

While there have been significant improvements in collecting data for intelligence purposes, the analysis of these data has been largely manual. This factor may have contributed to the lack of timely intelligence at the tactical level in the 1991 Gulf War. Research has provided evidence of the value of expert system techniques for intelligence processing and analysis in a conventional conflict setting and work is now being extended to a wider range of settings.

6.7 Multi-national C3 System Test Capability

The Gulf War proved the power and utility of a well-organised multi-national force. Fundamental to the success of this operation was an effective multi-national C3 system. The interoperation of computer based C3 systems presents many challenges not least interoperability of standards and security issues. Many of these systems-level issues were identified during the Gulf War and are now being addressed. A multi-national test environment for C3 systems, supported by real communications, is high priority requirement to support further research in this area. TTCP is well placed to co-ordinate the development and operation of such a multi-national test capability.

6.8 Training

The most effective training for C3 staff is to use the actual systems they would use in a real situation – future C3 systems should have access to realistic scenarios. The challenge becomes more complex when multi-national operations are considered. Distributed war-gaming across national boundaries will be required for effective training.

For the foreseeable future an integral component of all C3 systems will be the human operator. Computers which have genuine intelligence and the ability to learn, if achievable, are many years from fruition. As systems develop and become more complex, the limiting factor will increasingly be the human-machine interface. Systems of the future must have interfaces which require little or no training and are intuitive to use. Ways to improve the representation of information must be developed. Tools to navigate and seek out information intuitively from distributed data sources are high priority requirements. Virtual reality systems offer promise in this field. These and other HCI issues will take greater prominence along with the increasing complexity of C3 systems.

REFERENCES & BIBLIOGRAPHY

REFERENCES

1. Dept of Defence *The Defence of Australia 1987* dated March 1987.

2. Dept of Defence *Australia's Strategic Planning in the 1990s* dated September 1992.

3. Dept of Defence *Strategic Review 1993* dated December 1993.

4. *Journal of Electronic Defense* dated August 1993.

5. A D Campen *The First Information War* AFCEA ISBN 0-916159-24-8 dated October 1992.

6. P Dibb *The Strategic Priorities for Australian Defence Industry* Dept of Defence dated November 1992.

7. US Office Of the Joint Chiefs of Staff *C4I for the Warrior* dated 1992.

8. Dept of Defence *The Defence Corporate Communications Plan* dated May 1991.

9. H R Booher *Manprint and Approaches to System Integration* ISBN 0-442-00383.8 dated 1990.

BIBLIOGRAPHY

1. J L Boyes *Issue in C3I Program Management* AFCEA ISBN 0-916159-02-7 dated 1984.

2. S J Andriole *Advanced Technology for C2 Systems Engineering* AFCEA ISBN 0-916159-22-1 dated Nov 1990.

3. C E McKnight *Control of Joint Forces* AFCEA ISBN 0-916159-19-1 dated October 1990.

4. Dept of Defence *The Future Role of DSTO in Enhancing Australian Industry Capability* dated November 1992.

5. G Evans *Co-operating for Peace – The Global Agenda for the 1990s and Beyond* ISBN 1 86373 623 9 dated 1993.

6. V C Sobolewski *Towards a C3I Strategic Plan – Phase 1 Preliminary Considerations* ERL-0573-RE dated February 1993.

DISTRIBUTION LIST

	No. of Copies
FORCES EXECUTIVE	
ACDEV (F-3-3-0)	1 copy
ACOPS (M-B-42)	1 copy
DGDFPP (F-3-22)	1 copy
DGMSC (F-3-17)	1 copy
DGFD(Joint) (B-3-22)	1 copy
DGFD(SEA) (B-4-05A)	1 copy
DGFD(AIR) (B-1-06)	1 copy
DGFD(LAND) (B-3-01)	1 copy
DGJCE (M-SB-43)	1 copy
DGJOP (M-B-11)	1 copy
DOIS (B-2-29)	1 copy
DCJHQP (CP4-1-04)	1 copy
COFS CJFA(D)/DGJEP (H-2-43)	1 copy
ADFA Computer Science Dept	1 copy
NAVY OFFICE	
ACMAT-N (CP2-6-13)	1 copy
Naval Scientific Adviser (A-1-06)	1 copy
DIS-N (A-2-04)	1 copy
ARMY OFFICE	
ACMAT-A (J-2-Exec Suite)	1 copy
COMD EDE (Maribyrnong)	1 copy
DGMAT-A (J-2-Exec Suite)	1 copy
Scientific Adviser, Army (G-1-67)	1 copy
DCIS-A (G-1-42)	1 copy
DCCP-A (J-2-06)	1 copy
AIR FORCE OFFICE	
ACMAT-AF (F-2-58)	1 copy
DCAS (A-8-25)	1 copy
Air Force Scientific Adviser (C-4-28)	1 copy
DCIS-AF (A-6-20)	1 copy
STRATEGY AND INTELLIGENCE	
ADQ (M-3-61)	1 copy
DGIS (L-2-17)	1 copy
ASSA (L-2-15)	1 copy
DPCC (F-2-36)	1 copy

ACQUISITION AND LOGISTICS

FASDM (APW2-4-07)	1 copy
ASPPE (F-1-42)	1 copy
ASCISE (APW2-1-01)	1 copy
PDJP2030 (M-B-25)	1 copy
PDADFDIS (L-3-04)	1 copy
DISD (APW2-1-02)	1 copy
DCCCS (F-1-53)	1 copy

SCIENCE AND TECHNOLOGY

Chief Defence Scientist (APW1-3-03)	1 copy
Central Office Executive	1 shared copy
Senior Defence Scientific Adviser (G-1-66)	1 copy
Scientific Adviser POLCOM (APW2-3-17)	1 copy
Counsellor, Defence Science, London	Control Sheet
Counsellor, Defence Science, Washington	Control Sheet
Director, Electronics & Surveillance Research Laboratory	1 copy
Director, Aeronautical & Maritime Research Laboratory	1 copy
Chief Information Technology Division	1 copy
Chief Communications Division	1 copy
Chief Electronic Warfare Division	1 copy
Chief Guided Weapons Division	1 copy
Chief Land, Space and Optoelectronics Division	1 copy
Chief High Frequency Radar Division	1 copy
Chief Microwave Radar Division	1 copy
Chief Air Operations Division	1 copy
Chief Maritime Operations Division	1 copy
Research Leader Command & Control and Intelligence Systems	1 copy
Research Leader Military Computing Systems	1 copy
Research Leader Command, Control and Communications	1 copy
Research Leader Military Communications	1 copy
Research Leader Secure Communications	1 copy
Manager Human Computer Interaction Laboratory	Control Sheet
Head, Command Support Systems Group	1 copy + 20 spares
Head, Intelligence Systems Group	1 copy
Head, Communications Integration Group	1 copy
Head, C3I Systems Engineering Group	1 copy
Head, Program and Executive Support	Control Sheet
Head Software Engineering Group	1 copy
Head, Trusted Computer Systems Group	1 copy
Head, Systems Simulation and Assessment Group	1 copy
Head, Exercise Analysis Group	1 copy
Head, Computer Systems Architecture Group	1 copy
Head, Information Management Group	1 copy
Head, Information Acquisition & Processing Group	1 copy
Author	1 copy + 2 spares
Publications & Publicity Officer ITD	1 copy

LIBRARIES AND INFORMATION SERVICES

Australian Government Publishing Service	1 copy
Defence Central Library, Technical Reports Centre	1 copy
Manager, Document Exchange Centre, (for retention)	1 copy
National Technical Information Service, United States	2 copies
Defence Research Information Centre, United Kingdom	2 copies
Director Scientific Information Services, Canada	1 copy
Ministry of Defence, New Zealand	1 copy
National Library of Australia	1 copy
Defence Science and Technology Organisation Salisbury, Research Library	2 copies
Library Defence Signals Directorate Canberra	1 copy
British Library Document Supply Centre	1 copy
Parliamentary Library of South Australia	1 copy
The State Library of South Australia	1 copy

SPARES

Defence Science and Technology Organisation Salisbury, Research Library	6 copies

REPORT NO. DSTO-Task-Report-0002	AR NO. AR-008-908	REPORT SECURITY CLASSIFICATION Unclassified

TITLE

Trends in C3 system technology

AUTHOR(S)
K. Fairs

CORPORATE AUTHOR
Electronics and Surveillance Research Laboratory
DSTO Salisbury
Salisbury SA 5108

REPORT DATE July 1994	TASK NO. ADF 93/275	SPONSOR DOIS
FILE NO.	REFERENCES	PAGES 100

CLASSIFICATION/LIMITATION REVIEW DATE

CLASSIFICATION/RELEASE AUTHORITY

SECONDARY DISTRIBUTION

Approved for public release

ANNOUNCEMENT

Announcement of this report is unlimited

KEYWORDS

Command & Control
C3 Systems
Communications Networks
C3 Architectures

ABSTRACT

This paper gives an overview of technologies considered pertinent to Command, Control and Communications (C3) systems within the next 15 years. The style of the document is tailored deliberately for the non-specialist community. The report draws primarily from research being conducted within DSTO, and mentions significant world trends. The report discusses significant near-term issues influencing C3 system design. It proposes the functionality and architecture for a future C3 system, and then maps the technologies which could support migration to such a proposed future C3 system.